

全国计算机技术与软件专业技术资格（水平）考试参考用书

# 网络管理员考试同步辅导 (网络系统管理与维护篇)

全国计算机技术与软件专业技术资格（水平）考试办公室推荐

张伍荣 陶安 李文龙 施宁 主编



清华大学出版社



全国计算机技术与软件专业技术资格（水平）考试参考用书

# 网络管理员考试同步辅导

## （网络系统管理与维护篇）

全国计算机技术与软件专业技术资格（水平）考试办公室推荐

张伍荣 陶 安 李文龙 施 宁 主编

清华大学出版社

北京

[www.TopSage.com](http://www.TopSage.com)



# 全国计算机技术与软件专业资格(水平)考试真题及答案

[2008年下半年试题分析与解答 软考指定用书 清华出版](#)(含各科)

[2008年上半年试题分析与解答 软考指定用书 清华出版](#)(含各科)

[2007年下半年试题分析与解答 软考指定用书 清华出版](#)(含各科)

[2007年上半年试题分析与解答 软考指定用书 清华出版](#)(含各科)

[2006年下半年试题分析与解答 软考指定用书 清华出版](#)(含各科)

[2006年上半年试题分析与解答 软考指定用书 清华出版](#)(含各科)

[2009年计算机技术与软件水平考试各科目考试大纲汇总](#)

[全国计算机技术与软件专业资格\(水平\)考试真题及答案汇总](#)

[\[软考视频\]计算机技术与软件专业资格考试推荐视频教程下载汇总](#)

教材及同步辅导见下页。



# 计算机技术与软件专业技术(水平)考试指定教材及同步辅导

## 软考初级:

[程序员教程\(第二版\)2007 版 软考指定用书 高清PDF版](#)

[程序员考试辅导: 全国计算机技术与软件专业技术资格\(水平\)考试辅导用书](#)

[网络管理员教程\(第 2 版\)2007 版 软考指定用书 高清PDF版](#)

[网络管理员考试同步辅导\(计算机与网络基础知识篇\) 软考指定辅导用书](#)

[网络管理员考试同步辅导\(网络系统管理与维护篇\) 软考指定使用辅导用书](#)

## 软考中级:

[网络工程师教程\(第 2 版\) 2007 版 软考指定用书 高清PDF版](#)

[网络工程师教程 软考指定用书 高清PDF版](#)

[网络工程师考试同步辅导: 计算机与网络知识篇 软考指定用书](#)

[网络工程师考试同步辅导\(网络系统设计与管理篇\) 软考指定辅导用书](#)

[软件设计师教程\(第 2 版\) 2007 版 软考指定用书 高清PDF版](#)

[软件设计师考试同步辅导\(下午科目\) 高清PDF版](#)

[软件设计师考试同步辅导\(上午科目\) 高清PDF版](#)

[软件设计师考试考点分析与真题详解\(软件设计技术篇\)](#)

[软件设计师考试辅导: 考点精讲、例题分析、强化训练 冶金工业出版](#)

[数据库系统工程师教程 软考指定用书 高清PDF版](#)

[软件评测师教程 软考指定教材 高清PDF版](#)



[信息系统管理工程师教程 软考指定用书 高清PDF版](#)

[信息系统监理师教程 软考指定用书 高清PDF版](#)

软考高级:

[系统分析师教程 软考指定教材 高清PDF版](#)

[系统分析师考试辅导\(2007 版\) 软考指定辅导用书 高清PDF版](#)

[系统分析师教程 PDF文字版](#)

[系统分析师经典教材 Word版](#)

[信息系统项目管理师教程 软考指定教材 高清PDF版](#)

[信息系统项目管理师辅导教程\(上下册\)](#)

[计算机专业英语教程 PDF文字版](#)

更多计算机资料请访问: [大家论坛计算机专区](#)



## 内 容 简 介

本书是按照人事部、信息产业部 2004 年颁布的全国计算机技术与软件专业技术资格(水平)考试大纲(网络管理员级)和指定教材编写的考试辅导书。全书共分 6 章,内容包括小型计算机局域网的构建,综合布线,小型计算机局域网服务器配置,Web 网站建设,网络系统的运行、维护和管理,网络安全技术等。本书通过大纲要求、考点辅导、典型例题分析、本章小结和达标训练等几方面内容加以系统阐述。

本书具有考点分析透彻、例题典型、习题丰富、难度适中等特点,非常适合参加网络管理员级考试的考生使用,也可作为高等院校或培训班的教材。

版权所有,翻印必究。举报电话:010-62782989 13501256678 13801310933

本书扉页为防伪页,封面贴有清华大学出版社防伪标签,无上述标识者不得销售。

本书防伪标签采用特殊防伪技术,用户可通过在图案表面涂抹清水,图案消失,水干后图案复现;或将表面膜揭下,放在白纸上用彩笔涂抹,图案在白纸上再现的方法识别真伪。

### 图书在版编目(CIP)数据

网络管理员考试同步辅导(网络系统管理与维护篇)/张伍荣,陶安,李文龙,施宁主编. —北京:清华大学出版社, 2005.8

(全国计算机技术与软件专业技术资格(水平)考试参考用书)

ISBN 7-302-11503-6

I.网… II.①张… ②陶… ③李… ④施… III. ①计算机网络—系统管理—工程技术人员—资格考核—自学参考资料②计算机网络—维护—工程技术人员—资格考核—自学参考资料 IV.TP393

中国版本图书馆 CIP 数据核字(2005)第 087667 号

出 版 者: 清华大学出版社      地      址: 北京清华大学学研大厦  
<http://www.tup.com.cn>      邮      编: 100084  
社 总 机: 010-62770175      客户服务: 010-62776969

组稿编辑: 章忆文

文稿编辑: 刘    颖

封面设计: 孟繁聪

排版人员: 房利萍

印 刷 者: 北京国马印刷厂

装 订 者: 北京市昌平环球印刷厂

发 行 者: 新华书店总店北京发行所

开    本: 185×260    印张: 22.75    防伪页: 1    字数: 539 千字

版    次: 2005 年 8 月第 1 版    2005 年 12 月第 2 次印刷

书    号: ISBN 7-302-11503-6/TP·7551

印    数: 5001 ~ 7500

定    价: 34.00 元



## 前 言

全国计算机技术与软件专业技术资格(水平)考试自实施起至今已经历了十多年,在社会上产生了很大的影响,其权威性得到社会各界的广泛认可。为了适应我国信息化发展的需求,国家人事部和信息产业部决定将考试的级别拓展到计算机技术与软件各个方面,将网络程序员级别考试改为网络管理员级别考试,以满足社会上对各种信息技术人才的需要。为了帮助考生复习迎考,本书以 2004 年网络管理员考试大纲为依据,参照全国计算机技术与软件专业技术资格(水平)考试指定用书——《网络管理员教程》的结构进行编排,兼顾网络技术发展和知识更新,细化各章节的基础知识点,配以真题与典型例题并加以详细剖析。

2004 年网络管理员考试大纲与原来网络程序员的考试大纲在下午考试要求上有很大的变化,由原来的以网络编程基础知识为主变得更加多元化,更侧重于网络管理和维护知识的考查。本书的章节与 2004 年网络管理员考试大纲考试科目 2——网络系统的管理与维护基本一致,同时为了便于考生复习,对属于大纲要求的知识点但指定教材没有阐述的部分进行了必要的补充。书中的每一小节都分 4 个模块:考点辅导、典型例题分析、同步练习和同步练习参考答案。其中考点辅导部分主要以专题的方式,重点介绍网络管理员下午考试所需要的各个方面的知识,典型例题分析是本书的重点,书中的例题一部分是历次网络程序员、网络设计师和 2004 年下半年网络管理员考试真题,一部分是根据最新考试大纲精心设计而成的,具有典型性和代表性,所有例题均给出所考知识点及其详尽的分析。每章最后均配有本章小结和一定数量的习题和答案,对读者所学的知识 and 能力起到巩固、拓宽和提高作用。

全书共 6 章。第 1 章 小型计算机局域网的构建,第 2 章 综合布线,第 3 章 小型计算机局域网服务器配置,第 4 章 Web 网站建设,第 5 章 网络系统的运行、维护和管理,第 6 章 网络安全技术。

本书由张伍荣、陶安、李文龙、施宁主编。其中第 1 章、第 2 章由陶安编写,第 3 章、第 5 章由张伍荣编写,第 4 章由李文龙和俞永达编写,第 6 章由陶安和施宁编写。

在本书编写过程中,参考了许多相关书籍和资料,在此谨向这些参考文献的作者表示深深的谢意。

由于水平有限,时间也比较仓促,尽管经过多次校对和反复修改,书中难免存在错漏和不妥之处,敬请广大读者和专家批评指正。

编 者





# 目 录

## 第 1 章 小型计算机局域网的构建 ..... 1

### 1.1 局域网组网设计 ..... 1

#### 1.1.1 考点辅导 ..... 1

#### 1.1.2 典型例题分析 ..... 3

#### 1.1.3 同步练习 ..... 4

#### 1.1.4 同步练习参考答案 ..... 4

### 1.2 局域网组网技术及设备选择 ..... 5

#### 1.2.1 考点辅导 ..... 5

#### 1.2.2 典型例题分析 ..... 25

#### 1.2.3 同步练习 ..... 38

#### 1.2.4 同步练习参考答案 ..... 39

### 1.3 以太网交换机的部署、 配置和管理 ..... 42

#### 1.3.1 考点辅导 ..... 42

#### 1.3.2 典型例题分析 ..... 44

#### 1.3.3 同步练习 ..... 45

#### 1.3.4 同步练习参考答案 ..... 45

### 1.4 VLAN 的划分 ..... 47

#### 1.4.1 考点辅导 ..... 47

#### 1.4.2 典型例题分析 ..... 49

#### 1.4.3 同步练习 ..... 54

#### 1.4.4 同步练习参考答案 ..... 55

### 1.5 本章小结 ..... 55

### 1.6 达标训练题及参考答案 ..... 55

#### 1.6.1 达标训练题 ..... 55

#### 1.6.2 参考答案 ..... 57

## 第 2 章 综合布线 ..... 61

### 2.1 综合布线 ..... 61

#### 2.1.1 考点辅导 ..... 61

#### 2.1.2 典型例题分析 ..... 66

#### 2.1.3 同步练习 ..... 71

#### 2.1.4 同步练习参考答案 ..... 72

### 2.2 本章小结 ..... 73

### 2.3 达标训练题及参考答案 ..... 73

#### 2.3.1 达标训练题 ..... 73

#### 2.3.2 参考答案 ..... 73

## 第 3 章 小型计算机局域网 服务器配置 ..... 74

### 3.1 IP 地址及其规划 ..... 74

#### 3.1.1 考点辅导 ..... 74

#### 3.1.2 典型例题分析 ..... 84

#### 3.1.3 同步练习 ..... 90

#### 3.1.4 同步练习参考答案 ..... 92

### 3.2 DNS 服务器配置 ..... 93

#### 3.2.1 考点辅导 ..... 93

#### 3.2.2 典型例题分析 ..... 110

#### 3.2.3 同步练习 ..... 115

#### 3.2.4 同步练习参考答案 ..... 116

### 3.3 电子邮件服务 ..... 116

#### 3.3.1 考点辅导 ..... 116

#### 3.3.2 典型例题分析 ..... 130

#### 3.3.3 同步练习 ..... 132

#### 3.3.4 同步练习参考答案 ..... 133

### 3.4 FTP 服务器 ..... 133

#### 3.4.1 考点辅导 ..... 133

#### 3.4.2 典型例题分析 ..... 147

#### 3.4.3 同步练习 ..... 150

#### 3.4.4 同步练习参考答案 ..... 152

### 3.5 WWW 服务器配置 ..... 152

#### 3.5.1 考点辅导 ..... 152

#### 3.5.2 典型例题分析 ..... 159

#### 3.5.3 同步练习 ..... 161

#### 3.5.4 同步练习参考答案 ..... 162

### 3.6 代理服务器配置 ..... 163

#### 3.6.1 考点辅导 ..... 163

#### 3.6.2 典型例题分析 ..... 183

#### 3.6.3 同步练习 ..... 186

3.6.4 同步练习参考答案.....	188	5.1.3 同步练习 .....	291
3.7 DHCP 服务器配置 .....	188	5.1.4 同步练习参考答案 .....	291
3.7.1 考点辅导 .....	188	5.2 网络故障 .....	292
3.7.2 典型例题分析 .....	220	5.2.1 考点辅导 .....	292
3.7.3 同步练习 .....	224	5.2.2 典型例题分析 .....	297
3.7.4 同步练习参考答案 .....	225	5.2.3 同步练习 .....	299
3.8 本章小结 .....	225	5.2.4 同步练习参考答案 .....	299
3.9 达标训练题及参考答案 .....	226	5.3 数据备份与恢复 .....	299
3.9.1 达标训练题 .....	226	5.3.1 考点辅导 .....	299
3.9.2 参考答案 .....	234	5.3.2 典型例题分析 .....	316
<b>第 4 章 Web 网站建设 .....</b>	<b>237</b>	5.3.3 同步练习 .....	317
4.1 使用 HTML 制作网页 .....	237	5.3.4 同步练习参考答案 .....	318
4.1.1 考点辅导 .....	237	5.4 系统性能分析 .....	318
4.1.2 典型例题分析 .....	248	5.4.1 考点辅导 .....	318
4.1.3 同步练习 .....	255	5.4.2 典型例题分析 .....	324
4.1.4 同步练习参考答案 .....	257	5.4.3 同步练习 .....	326
4.2 网页制作工具 .....	258	5.4.4 同步练习参考答案 .....	326
4.2.1 考点辅导 .....	258	5.5 本章小结 .....	326
4.2.2 典型例题分析 .....	266	5.6 达标训练题及参考答案 .....	327
4.2.3 同步练习 .....	267	5.6.1 达标训练题 .....	327
4.2.4 同步练习参考答案 .....	268	5.6.2 参考答案 .....	328
4.3 动态网页制作 .....	269	<b>第 6 章 网络安全技术 .....</b>	<b>329</b>
4.3.1 考点辅导 .....	269	6.1 网络病毒防护策略 .....	329
4.3.2 典型例题分析 .....	277	6.1.1 考点辅导 .....	329
4.3.3 同步练习 .....	279	6.1.2 典型例题分析 .....	331
4.3.4 同步练习参考答案 .....	280	6.1.3 同步练习 .....	331
4.4 Web 网站的创建与维护 .....	280	6.1.4 同步练习参考答案 .....	331
4.4.1 考点辅导 .....	280	6.2 防火墙的配置策略 .....	331
4.5 本章小结 .....	281	6.2.1 考点辅导 .....	331
4.6 达标训练题及参考答案 .....	282	6.2.2 典型例题分析 .....	336
4.6.1 达标训练题 .....	282	6.2.3 同步练习 .....	339
4.6.2 参考答案 .....	285	6.2.4 同步练习参考答案 .....	339
<b>第 5 章 网络系统的运行、 维护和管理 .....</b>	<b>287</b>	6.3 入侵处理策略 .....	340
5.1 网络管理软件 .....	287	6.3.1 考点辅导 .....	340
5.1.1 考点辅导 .....	287	6.3.2 典型例题分析 .....	344
5.1.2 典型例题分析 .....	290	6.3.3 同步练习 .....	347
		6.3.4 同步练习参考答案 .....	347
		6.4 漏洞处理策略 .....	348

6.4.1 考点辅导.....	348	6.6 达标训练题及参考答案.....	350
6.4.2 典型例题分析.....	349	6.6.1 达标训练题 .....	350
6.4.3 同步练习.....	349	6.6.2 参考答案 .....	351
6.4.4 同步练习参考答案.....	349	参考文献 .....	353
6.5 本章小结.....	350		



Q11.....	Q12.....
Q13.....	Q14.....
Q15.....	Q16.....
Q17.....	Q18.....
Q19.....	Q20.....

# 第1章 小型计算机局域网的构建

大纲要求:

- 组网设计
- 组网技术选择
- 组网设备选择及部署
- 设备配置和管理
- 划分 VLAN

## 1.1 局域网组网设计

### 1.1.1 考点辅导

#### 1.1.1.1 设计原则

设计局域网时, 应遵循以下原则:

##### 1. 实用性原则

网络系统应采用成熟可靠的技术和设备, 这样才能做到实用、经济和有效。

##### 2. 开放性原则

网络系统应采用开放的标准和技术。

##### 3. 可靠性原则

网络系统应确保很高的可靠性, 具有较高的平均无故障时间和较低的平均故障率。

##### 4. 安全性原则

网络系统应具有良好的安全性, 确保网络系统和数据的安全运行。

##### 5. 先进性原则

网络系统应采用先进的技术和设备, 符合网络未来发展的潮流。

##### 6. 高效性原则

网络系统应具有很高的资源利用率。

##### 7. 可扩展性原则

网络系统应在规模和性能两方面具有良好的可扩展性。

##### 8. 高性价比原则

网络系统应具有较高的性能价格比, 技术优先, 兼顾价格。

### 1.1.1.2 局域网设计的步骤

#### 1. 网络需求分析

在组建局域网之前首先要进行需求分析工作, 根据用户提出的要求, 进行网络设计, 网络建设的成败很大一部分取决于网络实施前的规划工作。

##### (1) 网络的功能要求

任何网络都不可能是一个能够满足各项功能需求的“万能网”。因此, 必须针对每个具体的网络所要完成的功能, 依据使用需求、实现成本、未来发展、总预算投资等因素对网络的组建方案进行认真的设计和推敲。

##### (2) 网络的性能要求

根据对网络系统处理的性能进行分析。根据网络的工作站权限、容错程度、网络安全性等方面等要求, 确定采取何种措施及方案。

##### (3) 网络运行环境的要求

根据整个局域网运行时所需要的环境要求, 确定使用哪种网络操作系统、应用软件和共享资源。

##### (4) 网络的可扩充性和可维护性要求

如何增加工作站、怎样与其他网络联网、对软件/硬件的升级换代有何要求与限制等, 都要在网络设计时加以考虑, 以保证网络的可扩充性和可维护性。

#### 2. 确定网络类型和带宽

与其他网络技术相比, 以太网具有价格低、可靠性高、可扩展性好、易于管理等优点。所以一般局域网都选择以太网。根据局域网接入计算机的数量及规模可确定网络带宽和交换设备, 目前快速以太网能够满足网络数据流量不是很大的中小型局域网的需要。但是在计算机数量达到数百台或网络数据流量比较大的情况下, 应采用千兆以太网技术, 以满足对网络主干数据流量的要求。网络主干和分支方案确定之后, 就可以选择集线器或交换机产品了。集线器或交换机的型号与数量由联入网络的计算机数量和网络拓扑结构来决定。

#### 3. 确定网络设备

网络设备选择应遵循以下原则:

##### (1) 厂商的选择

所有网络设备尽可能选取同一厂家的产品, 这样在设备可互连性、协议互操作性、技术支持、价格等方面更有优势。

##### (2) 扩展性考虑

在网络的层次结构中, 主干设备应预留一定的扩展能力, 而低端设备则够用即可, 因为低端设备更新较快, 且易于扩展。

##### (3) 根据方案实际需要选型

主要在参照整体网络设计要求的基础上, 根据网络实际带宽性能需求、端口类型和端口密度选型。如果是旧网改造项目, 则应尽可能保留并延长用户对原有网络设备的投资, 减少在资金投入方面的浪费。

#### (4) 选择性能价格比高、质量过硬的产品

为使资金的投入与产出达到最大值,能以较低的成本、较少的人员投入来维护系统运转,网络开通后,能运行许多关键业务,因而要求系统具有较高的可靠性。

#### 4. 确定布线方案和布线产品

现在的布线系统主要是光纤和非屏蔽双绞线,小型网络多以超五类非屏蔽双绞线为布线系统,因为布线是一次性工程,因此应考虑在未来几年内网络扩展的最大点数。

#### 5. 确定服务器和网络操作系统

服务器是网络数据储存的仓库,其重要性可想而知。服务器的类型和档次应与网络的规模和数据流量以及可靠性要求相匹配。

如果是几十台计算机以下的小型网络,并且数据流量不大,选用入门级服务器基本上可以满足需要;如果是数百台左右的中型网络,则应选用工作组级服务器;如果是上千台的大型网络,则应选用企业级服务器。

服务器的数量由网络应用来决定,可以根据实际情况,配备 E-mail 服务器、Web 服务器、数据库服务器等,也可以让一台服务器充当多种服务器角色。

目前,网络操作系统基本上是三分天下:微软的 Windows 2000 Server、传统的 Unix 和 Linux,可以根据网络规模、技术人员水平、资金等综合因素来决定究竟使用什么网络操作系统。

#### 6. 其他

局域网的设计还包括不间断电源、网络安全、互联网接入、网络应用系统等方面的设计。

### 1.1.2 典型例题分析

例 请简要回答如下局域网设计时的有关问题。

【问题 1】简述设计网络系统时需遵循的基本原则。

【问题 2】局域网的硬件设备目前大多选择什么网络设备。

【问题 3】以太网的特点是什么?

【问题 4】局域网设计与连接时考虑的主要因素是什么?

分析:设计局域网时,应遵循以下原则:实用性原则、开放性原则、可靠性原则、安全性原则、先进性原则、高效性原则、可扩展性原则、高性价比原则。

以太网技术是目前局域网技术中最成熟的技术。所以局域网的硬件设备大多选择以太网的网络设备。以太网的特点如下:

(1) 开放标准,获得众多厂商的支持。目前,几乎所有的硬件制造商生产的设备和几乎所有的软件开发商的操作系统和应用协议都与以太网兼容。

(2) 易于移植和升级,可最大限度保护用户投资。对于所有以太网技术,其帧的结构几乎是一样的,这就提供了非常好的升级途径。快速以太网技术提供了从 10Mb/s 向 100Mb/s 以太网的平滑升级。千兆和万兆以太网的出现,在增加带宽的同时也扩展了可升级性。只要将低速以太网设备用交换机连接到千兆或万兆以太网的设备上,就可实现一个物理线速



向另一物理线速的适配。这样的升级方式就使得千兆和万兆能无缝地与现在的以太网集成在一起。

(3) 价格便宜, 管理成本低。以太网技术无论在局域网、接入网还是即将进入的城域网、广域网在价格上与其他技术相比都具有优越性。若全面采用以太网解决方案, 价格将更具有吸引力。另外, 以太网存在时间长, 标准化程度高, 一般网络管理人员都比较熟悉, 因此它的运行维护管理成本也比较低。

(4) 结构简单, 组网方便。以太网技术的实现原理统一采用了 CSMA/CD 媒体访问控制方法, 不同版本的以太网的帧结构和网络拓扑结构也是一致的, 对布线系统的要求较低, 网络连接设备的配置比较简单。

所以一般局域网都选择以太网。根据局域网接入计算机的数量及规模可确定网络带宽和交换设备, 目前快速以太网能够满足网络数据流量不是很大的中小型局域网的需要。但是在计算机数量达到数百台或网络数据流量比较大的情况下, 应采用千兆以太网技术, 以满足对网络主干数据流量的要求。网络主干和分支方案确定之后, 就可以选定集线器或交换机产品了。集线器或交换机的数量由联入网络的计算机数量和网络拓扑结构来决定。

答案:

【问题 1】设计网络系统时应遵循: 实用性原则、开放性原则、可靠性原则、安全性原则、先进性原则、高效性原则、可扩展性原则、高性价比原则。

【问题 2】以太网。

【问题 3】以太网具有开放标准, 获得众多厂商的支持; 易于移植和升级, 最大限度保护用户投资; 价格便宜, 管理成本低; 结构简单, 组网方便等特点。

【问题 4】网络类型和带宽。

### 1.1.3 同步练习

1. 如何确定局域网的服务器? 局域网常使用的操作系统有哪些?
2. 简述选择网络设备应遵循的原则?

### 1.1.4 同步练习参考答案

1. 服务器是网络数据储存的仓库, 其重要性可想而知。服务器的类型和档次应与网络的规模和数据流量以及可靠性要求相匹配。如果是几十台计算机以下的小型网络, 而且数据流量不大, 选用入门级服务器基本上可以满足需要; 如果是数百台左右的中型网络, 选用工作组服务器; 如果是上千台的大型网络, 选用企业级服务器。

局域网常使用的操作系统有微软的 Windows 2000 Server、Unix 和 Linux。

2. 答案参见本节考点辅导部分。

## 1.2 局域网组网技术及设备选择

### 1.2.1 考点辅导

#### 1.2.1.1 局域网基础

##### 1. 局域网参考模型

局域网体系结构由物理层、媒体访问控制子层(MAC)和逻辑链路控制子层(LLC)组成。IEEE 802 参考模型的最底层对应于 OSI 模型中的物理层, 包括以下功能:

- (1) 信号的编码/解码。
- (2) 前导码的生成/去除(前导码仅用于接收同步)。
- (3) 位的发送/接收。

IEEE 802 参考模型的 MAC 子层和 LLC 子层合起来与 OSI 模型中的数据链路层相对应。

MAC 子层完成的功能如下:

- (1) 在发送时将要发送的数据帧组装成帧, 帧中包含有地址和差错检测等字段。
- (2) 在接收时, 将接收到的帧解包, 进行地址识别和差错检测。
- (3) 管理和控制对于局域网的传输媒体的访问。

LLC 子层完成的功能如下:

(1) 为高层协议提供相应的接口, 即一个或多个服务访问点(SAP), 通过 SAP 支持面向连接的服务和复用能力。

- (2) 端到端的差错控制和确认, 保证无差错传输。
- (3) 端到端的流量控制。

需要指出的是, 在局域网中采用了两级寻址, 用 MAC 地址标识局域网中的一个站, LLC 提供了服务访问点(SAP)地址, SAP 指定了运行于一台计算机或网络设备上的一个或多个应用进程地址。

##### 2. 局域网拓扑结构

按照不同的物理布局, 局域网的拓扑结构通常可分为 3 种, 分别是总线拓扑结构、星型拓扑结构和环型拓扑结构。

总线结构是使用同一媒体或电缆连接所有端用户的一种方式, 也就是说, 连接端用户的物理媒体由所有设备共享。

星型结构有中心节点, 各节点通过点对点的方式与中心节点相连, 任何两个节点之间的通信都要通过中心节点来转接。

环型结构在 LAN 中使用较多。这种结构的传输媒体从一个端用户连接到另一个端用户, 直到将所有端用户连成环型。

##### 3. 局域网媒体访问控制方法

目前, 计算机局域网常用的访问控制方式有 3 种, 分别是载波侦听多路访问/冲突检测

(CSMA/CD), 令牌环访问控制法(Token Ring)和令牌总线访问控制法(Token Bus)。

CSMA/CD 包含两方面内容: 即载波侦听(CSMA)和冲突检测(CD)。CSMA/CD 访问控制方式主要用于总线型网络拓扑结构, 是 IEEE 802.3 局域网标准的主要内容。

Token Ring 是令牌通行环的简写。其主要技术指标是: 网络拓扑为环型布局, 基带网, 数据传送速率为 4Mb/s, 采用单个令牌(或双令牌)的令牌传递方法。环型网络的主要特点是: 只有一条环路, 信息单向沿环流动, 无路径选择问题。

Token Bus 是令牌通行总线(Token Passing Bus)的简写。这种方式主要用于总线型或树型网络结构中。1976 年美国 Data Point 公司研制成功的 ARCnet(Attached Resource Computernetwork)网络, 它综合了令牌传递方式和总线网络的优点, 在物理总线结构中实现令牌传递控制方法从而构成一个逻辑环路。此方式也是目前计算机局域网中的主流介质访问控制方式。

### 1.2.1.2 无线局域网简介

#### 1. 无线数据网络的种类

无线数据网络解决方案包括: 无线个人网、无线局域网、无线城域网和无线广域网。

无线个人网主要用于个人用户工作空间, 典型的覆盖距离为几米, 可与计算机同步传输文件, 访问本地外围设备, 通常被形容为满足“最后 10 米”的通信需求, 目前的主要技术为蓝牙(Bluetooth)技术。

无线局域网(WLAN, Wireless LAN)是一种借助于无线技术取代有线布线方式构成局域网的新手段。WLAN 可提供传统有线局域网的所有功能, 是计算机网络与无线通信技术相结合的产物。目前, WLAN 领域主要是 IEEE 802.11X 标准系列, 其中应用最为广泛的是 IEEE 802.11b。

无线城域网是一种有效作用距离比 WLAN 更远的宽带无线接入网络, 通常用于城市范围内的业务点和信息汇聚点之间的信息交流和网际接入。有效覆盖区域为 2~10km, 最大可达 30km, 数据传输率最快可达 70Mb/s, 目前, 主要的技术标准是 IEEE 802.16 系列。

无线广域网(WWAN, Wireless WAN)主要用于满足一个城市范围的信息交流无线接入需求。IEEE 802.20 和 3G 蜂窝移动通信系统是 WWAN 的主要标准。

#### 2. 无线局域网的扩频技术

无线局域网采用电磁波作为载体传送数据信息, 使用的模式主要是窄带和扩频。目前无线局域网的数据传输通常采用无线扩频技术 SST(Spread Spectrum)。常见的扩频技术包括两种: 跳频扩频(FHSS, Frequency-Hopping Spread Spectrum)和直接序列扩频(DSSS, Direct Sequence Spread Spectrum), 它们工作在 ISM 频段(Industrial Scientific Medical Band)上。

#### 3. 无线局域网的拓扑结构

无线局域网分为对等网络和结构化网络两种拓扑结构。

对等网络(Peer to Peer)用于一台计算机(无线工作站)和另一台或多台计算机(其他无线工作站)的直接通信, 该网络无法接入有线网络中, 只能独立使用。对等网络中的一个节点必须能“看”到网络中的其他节点, 否则就认为网络中断, 因此对等网络只适应于少数用户的组网环境, 并且距离足够近。

结构化网络(Infrastructure)由无线访问点(AP, Access Point)、无线工作站(STA, Station)以及分布式系统(DSS)构成,覆盖的区域分为基本服务区(BSS, Basic Service Set)和扩展服务区(ESS, Extended Service Set)。

#### 4. 无线局域网的主要工作过程

无线局域网的主要工作过程包括:扫频、关联、重关联和漫游。

#### 5. 无线局域网的访问控制方式

IEEE 802.11b 标准的无线局域网使用的是带冲突避免的载波侦听多路访问方法(CSMA/CA)。

### 1.2.1.3 10Mb/s 以太网

10Mb/s 以太网一般指速率小于或等于 10Mb/s 的低速以太网。根据传输介质的不同,10Mb/s 以太网大致有 4 个标准,各个标准的 MAC 子层媒体访问控制方法和帧结构以及物理层的编码方法(曼彻斯特编码)均是相同的,不同的是传输媒体和物理层的收发器及媒体连接方式,按照技术出现的时间顺序,这 4 个标准依次是:

#### 1. 粗缆以太网(10Base5)

10Base5 采用 RG-11 型粗同轴电缆为传输介质,其阻抗为  $50\Omega$ ,直径为 0.4in。在 10Base5 中,每个计算机节点都通过网卡(AUI 接口)、收发器电缆(AUI Cable)和“收发器”与总线相连,如图 1.1 所示。

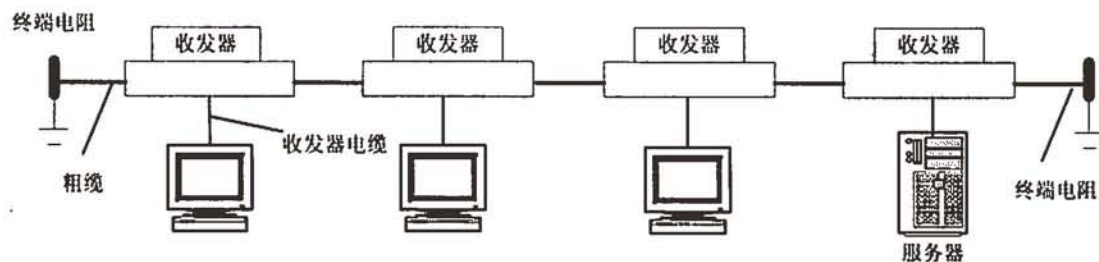


图 1.1 10Base5 网络结构

10Base5 代表的具体意思是:工作速率 10Mb/s,采用基带信号,每一个网段的最长为 500m。

通常在标准以太网网络接口板上提供一个 15 针的 AUI(DIX)接口,收发器电缆采用  $78\Omega$  的 6 对屏蔽双绞线电缆,将收发器与 PC 机网卡连接,粗同轴电缆两端接上  $50\Omega$  的终端匹配器(也叫端接器),其中之一必须接地,这就构成了网络段,每段最远距离为 500 米。一个粗缆以太网最多可以有 5 段。电缆最大距离是 2500m,工作站之间的最小距离为 2.5m,收发器电缆最长距离是 50m。

#### (1) 硬件基本配置

网卡:联网的每个节点都需要一块带有 15 针 AUI(DIX)接口的 10Mb/s 网卡。

收发器:粗缆以太网的每个节点需要通过一个安装在总线同轴电缆上的外部收发器(带有 15 针的 AUI 接口)联入网内。

收发器同轴电缆(AUI 电缆):用于节点中网卡与收发器的连接。



电缆系统: RG-11 型 50 $\Omega$  粗同轴电缆, 终端电阻安装在电缆的两端, 防止信号的反射, 其中之一必须接地。

中继器: 主要用来扩展作为总线的同轴电缆长度和工作站(节点)个数。

### (2) 主要技术参数

在粗缆以太网中, 不使用中继器时, 每段粗缆的最大距离为 500m。如果使用中继器, 应遵循 5-4-3 规则, 即一个粗缆以太网中最多允许使用 4 个中继器, 连接 5 段最大长度为 500m 的粗同轴电缆; 而 5 段中只有 3 段可以连接工作节点, 其余两段只能用于扩展网络距离。使用中继器后的粗缆以太网的最大长度不能超过 2500m; 由于每个以太网段中联入的节点数最多为 100 个, 最多可以有 3 个网段连接工作节点, 因此, 最多有 300 个工作节点; 两个相邻的收发器之间的最小距离为 2.5m, 收发器电缆最大长度为 50m。

### (3) 特点

优点: 可靠性高, 抗干扰能力强, 作用距离长。

缺点: 粗缆较贵, 而且要求每个工作站都配置一个外部收发器和收发器电缆, 因而成本较高、网络投资较大。

### (4) 主要技术规范

拓扑结构: 总线。

介质访问控制方法: CSMA/CD。

网络类型: RG-11 型 50 $\Omega$  粗同轴电缆。

传输速度: 10Mb/s。

最大网络节点数目: 300 个。

每段最大节点数目: 100 个。

最大网段数目: 5 个, 最多使用 4 个中继器, 其中 3 个网段可连接工作节点。

节点间最小距离: 2.5m。

最大网络长度: 2500m。

最大网段长度: 500m。

## 2. 细缆以太网(10Base2)

10Base2 使用 RG-58 型细缆、BNC-T 型连接器, 以线性总线进行布线。10Base2 将原来 10Base5 的收发器功能移植到网卡上, 因此, 使得网络的组建更简单, 性能价格比也比 10Base5 高, 然而, 却也因此限制了信号能够传送的最大距离。其结构如图 1.2 所示。

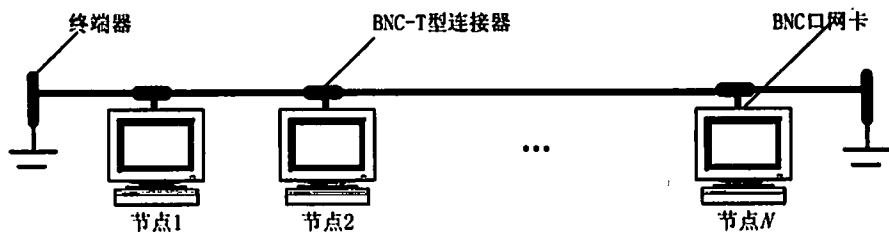


图 1.2 10Base2 网络结构

10Base2 代表的具体意思是: 工作速率为 10Mb/s, 采用基带信号, 每一个网段最长约为 200m。

一个细缆以太网的“单段”最大长度为 185m，最多可使用 4 个中继器，即可以有 5 个电缆段，而 5 段中只有 3 段可以连接工作节点，其余两段只能用于扩展网络距离。电缆总长度最大为 925m。一个网段中节点的最多数目为 30 个，因此，最多可以有 90 个工作节点。

两个相邻的 BNC-T 型连接器的最小距离是 0.5m，每段的两端都必须安装一个  $50\Omega$  终端匹配器，并且有一端应接地。网卡提供 BNC 接口，同轴细缆通过 T 型接头与网卡连接，所有 T 型接头必须直接接到工作站 BNC 接口上，中间不得接入任何电缆。

图 1.3 表示一个使用中继器扩展网络距离的双网段 10Base2 组网实例。

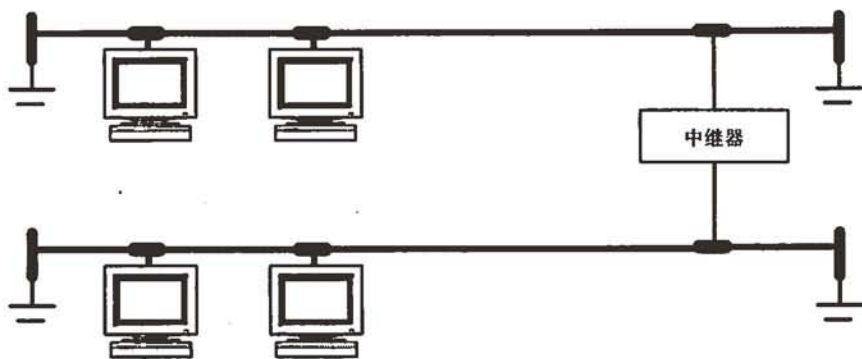


图 1.3 使用中继器连接的“双网段”10Base2 网络结构

#### (1) 硬件基本配置

网卡：带有 BNC 接口的 10Mb/s 网卡。

BNC-T 型连接器：细缆以太网中的每个节点通过 BNC-T 型连接器联入网内。

电缆系统：RG-58 型  $50\Omega$  细同轴电缆，终端电阻安装在电缆的两端，防止信号的反射，其中之一必须接地。

中继器：主要用来扩展作为总线的细轴电缆长度和工作站(节点)个数。

#### (2) 特点

优点：系统造价低廉，安装容易，具有最短的布线距离。

缺点：由于网段中联入多个 BNC-T 型连接器，存在着多个 BNC 型连接头和 BNC-T 型连接器的连接点，因而同轴电缆连接的故障率较高。

#### (3) 技术规范

拓扑结构：总线。

介质访问控制方法：CSMA/CD。

网络类型：RG-58 型  $50\Omega$  细同轴电缆。

传输速度：10Mb/s。

最大网络节点数目：90 个。

每段最大节点数目：30 个。

最大网段数目：5 个，最多使用 4 个中继器，其中 3 个网段可以连接工作节点。

节点间最小距离：0.5m。

最大网络长度：925m。

最大网段长度: 185 米。

### 3. 双绞线以太网(10 BaseT)

10BaseT 以太网是使用非屏蔽双绞线电缆来连接的传输速率为 10Mb/s 的以太网。10 BaseT 以太网支持结构化布线系统, 10BaseT 以太网需要使用集线器(Hub)构成总线或总线型和星型结合的混合型网络拓扑, 具有良好的故障隔离功能, 使得网络任一段线路或一工作站出现障碍时, 均不影响网络其他站点, 简化了网络故障诊断过程, 缩短了故障诊断时间, 提高了网络故障检测和冲突控制效率, 使局域网难于维护的缺点得以根本性改变。加之其组网容易, 使得 10BaseT 以太网成为目前使用最广的局域网系统。

10BaseT 代表的具体意思是: 工作速率为 10Mb/s, 采用基带信号, T 表示的是传输媒体双绞线。

单个集线器和多个集线器的 10BaseT 以太网连接如图 1.4 所示:

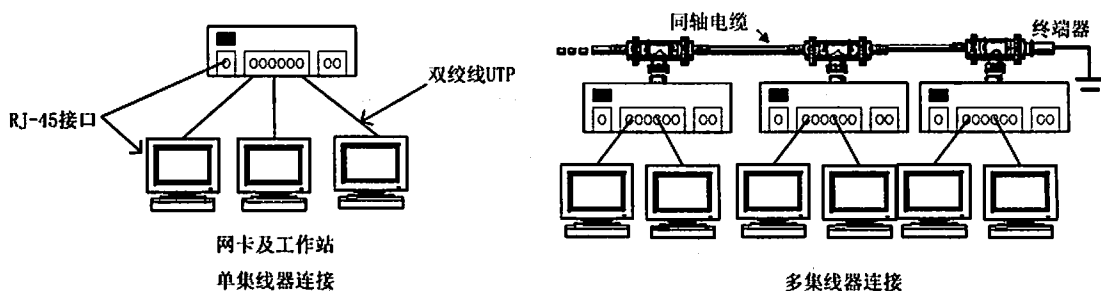


图 1.4 10BaseT 以太网连接

#### (1) 硬件基本配置

**集线器:** 集线器也就是 Hub, 是双绞线以太网的中心连接设备, 有多个 RJ-45 型接口, 能支持多个工作站(客户机)入网, Hub 上的 RJ-45(级联或普通)接口还可以与其他 Hub 相连, 易于扩展网络。Hub 上的 BNC 向上接口与 BNC-T 型连接器相接时, 可以与细缆以太网相连。Hub 上的 AUI 接口可以与粗缆以太网的收发器电缆相连。新型的高速 Hub 上还配有光纤接口, 通过此接口, 可以接入光纤主干线。

**非屏蔽双绞线:** 10BaseT 网络标准最低采用 3 类 UTP, 两端都装有同样的 RJ-45 型接头(水晶头), 每一个工作节点都需要一根双绞线电缆, 用来连接工作节点上的网卡与集线器。

**网卡:** 带有 RJ-45 接口的网卡。

#### (2) 双绞线以太网的扩展组网方案

使用集线器和双绞线的以太网结构分为: 单集线器结构、多集线器级联结构、叠加集线器结构。

##### ① 多集线器级联结构

对于规模较大, 或节点(工作站)数超过单集线器的端口数目时, 常采用多集线器的连接, 这就是集线器的“级联”。级联的目的是为了组成更大规模的网络, 级联结构的 10BaseT 网络也遵循 5-4-3 规则, 即任一条通路上的两台计算机间最多不能超过 5 段线, 即最多可以串联 4 个集线器; 这段线既包括集线器与集线器的连线, 也包括集线器到计算机间的连线。3 个集线器能连接设备, 2 个只能用于级联。网络上连接设备的总数不得超过 1024 台。在级联之前, 必须首先弄清集线器上的端口类型。

普通集线器提供的端口类型有以下3类:

- 用于连接节点(工作站或服务器)的普通 RJ-45 端口。
  - 专门用于双绞线以太网集线器的级联端口:即专门用于级联的“出口/入口”、或者是“Uplink”端口。
  - “向上连接端口”:这些端口可以连接粗缆的 AUI 端口,或细缆的 BNC 端口,也可以连接光纤端口。
- ② 对应于不同的端口,多集线器结构的级联有以下几种方法:
- 使用“标准线”,通过以太网集线器上专门的 RJ-45 型级联“出/入”端口进行级联。
  - 对于没有专门级联“出口/入口”的两个集线器,可以使用“标准线”将一个集线器上边的“Uplink”级联口与另一个集线器上边的普通 RJ-45 型端口相连,从而实现多集线器之间的级联。
  - 使用“交叉线”连接两个没有“级联(Uplink)”口的集线器上的普通 RJ-45 接口。也可以实现多集线器的级联。
  - 使用同轴电缆、光纤通过集线器提供的“向上连接端口”实现级联。

由于 10BaseT 以太网和粗、细缆以太网都属于 IEEE 802.3 规范,因此,互连十分方便。连接时,通常采用同轴电缆作为主干网,通过双绞线作为分支网络,这样可以提高干线的可靠性与干扰能力,并可延长传输距离。

利用集线器的“向上连接端口”进行级联,可以扩大局域网覆盖范围。例如如果使用细缆连接两个集线器,细缆的单根缆段的最大长度为 185m,那么两个 10BaseT 网络中节点的最大距离可达到 385(即,  $185+100+100$ )m。如果使用粗缆连接两个集线器,粗缆的单根缆段的最大长度为 500m,那么网中两节点最大距离可达到 700(即,  $500+100+100$ )m;如果在粗或细缆段中配合使用中继器,那么多缆段、多集线器级联系统的覆盖范围还可以更大。

### ③ 可叠加集线器以太网结构

可叠加集线器适用于中、小企业联网环境。可叠加集线器是由一个基础集线器与多个扩展集线器组成。基础集线器是一个具有网络管理功能的独立集线器。通过基础集线器,可以叠加多个扩展集线器,一方面可以增加以太网的节点(工作站)数目,另一方面可以实现对网中工作节点的网络管理功能。其结构图如图 1.5 所示。

### (3) 10BaseT 以太网的特点

#### ① 优点:

- 故障检测容易,当某一段线路、工作站或互连的某个 Hub 出现故障时,Hub 会将故障节点自动排除在网络之外,因而保证了剩余部分的正常工作。
- 安装、管理和使用都很简单。适于中小型单位自行组建局域网。
- 同时具有成本低、扩展方便、改变网络布局容易等优点。

#### ② 缺点:

- 这种结构的最大缺点在于它是一种共享介质的网络,随着网络节点的增加,冲突也会增加,网络的性能会随之急剧下降。有实验表明,一个单 Hub 的 10BaseT,虽然具有 10Mb/s 的带宽,但是,当网络工作节点增至 20 个的时候,其实际的可用带宽将降至原来的 30%~40%。此外,当使用多个 Hub(最多 4 个)级联时,或者



是与其他以太网连接之后,所有网络节点将共享 10Mb/s 的带宽。Hub 所连接的节点越多,每个工作节点得到的带宽就越窄。在高负荷时,网络性能将急剧下降,这是组建共享式以太网遇到的最大问题。

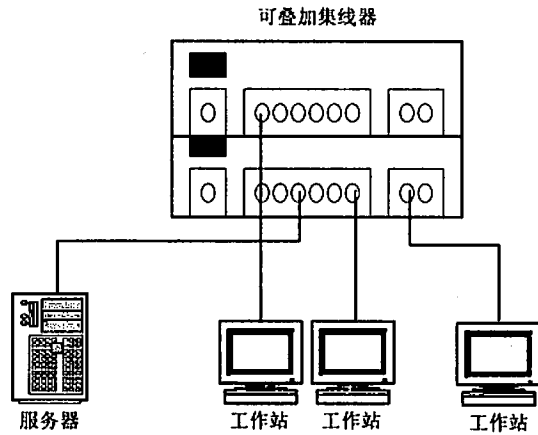


图 1.5 可叠加集线器以太网结构

- 网络的中央节点的负荷过重,一旦 Hub 出现故障,将导致整段或全部网络瘫痪。
- 双绞线的抗干扰能力弱。
- 由于每个单段网线只能连接一个工作节点,所以网络通信线路的利用率很低。

#### (4) 技术规范

**拓扑结构:** 由于介质访问控制方法为 CSMA/CD, 因此, 10BaseT 是逻辑上的“总线”型拓扑结构; 物理上的“星型”拓扑结构。

**网线类型:** 3、5 或超 5 类的非屏蔽双绞线。

**传输速度:** 10Mb/s。

**最大网络节点数目:** 1024 个。

**每段最大集线器数量:** 1 个。

**级联的最大集线器数量:** 4 个。

**最大网络长度:** 500m。

**最大网段长度:** 100m。

#### 4. 光纤以太网(10BaseF)

10BaseF 以太网传输媒体采用多模光纤, 拓扑结构为星型, 所有站点连接到一个支持光纤接口的中心集线器上, 每个电缆段的长度不能超过 2000 米。

10BaseF 以太网设计也遵循“5-4-3”法则, 但由于受 CSMA/CD 碰撞域的影响, 整个网络的最大跨距为 4000m。

10BaseF 代表的具体含义是: 工作速率为 10Mb/s, 采用基带信号, F 表示的是传输媒体光纤。

#### 1.2.1.4 快速以太网

##### 1. 快速以太网简介

快速以太网是在传统以太网的基础之上发展而来的,因此它不仅保持相同的以太网帧格式,而且还保存留了用于以太网的 CSMA/CD 媒体访问控制方式。由于快速以太网的速率比普通以太网提高了 10 倍,所以快速以太网中的网桥、路由器和交换机都与普通以太网不同,它们具有更快的速率和更短的延时。

目前正式的 100BaseT 标准定义了三种物理层规范以支持不同的物理介质,分别为:

- 100BaseTX 用于两对 5 类 UTP 或 1 类 STP
- 100BaseT4 用于四对 3、4 或 5 类 UTP
- 100BaseFX 用于光纤

其中 100BaseTX 规范描述如何通过 1 类屏蔽双绞线(STP)或者 5 类非屏蔽双绞线(UTP) 传送快速以太网帧,5 类 UTP 是目前使用最为广泛的介质,100BaseTX 标准使用其中两对,连接方法和 10BaseT 完全相同,其采用的拓扑结构为星型。这意味着不必改变布线格局可直接将 10BaseT 的布线系统移植到 100BaseTX 上。

100BaseT4 规范提出了 100BaseTX 在 3 类 UTP 上传送数据的具体规定,即 100BaseT4 使用四对 3、4 或 5 类 UTP,连接最大距离 100m。而 10BaseT 只使用两对线,因此老式的 3 类 UTP 布线的 10BaseT 系统必须改变端点上的电缆连线,才能正常运行 100BaseT4。

100BaseFX 是针对光纤提出的物理层规范,它的连线比 100BaseTX 长(450m),如果采用非标准的全双工模式连线长度可达 2km,单模光纤传输距离可达 40km。另外,抗干扰能力也大大优于 UTP 和 STP。

##### 2. 100BaseT 组网方法

目前大部分以太网系统都配置一台或多台服务器,在采用以太网/快速以太网交换技术升级组网时,可以将原以太网服务器的网卡更换为快速以太网卡(100BaseTX 网卡),并利用 5 类 UTP 通过 RJ-45 端子接入 100Mb/s 交换机的 100Mb/s 高速端口上。对于一般工作站,不必更换网卡,可通过原来的共享 Hub 集中连接到 100Mb/s 交换机级联的 10/100Mb/s 交换机的 10Mb/s 端口上,组成 10Mb/s 共享网。对于那些对带宽要求较高的数据库服务器,工作站以及打印机等,可单独连接到 10/100Mb/s 交换机的端口上,组成多级交换机的快速以太网,其连接方法如图 1.6 所示。

##### 3. 快速以太网的拓扑结构

100BaseT 除了在传输介质、网卡、工作站、Hub 以及服务器硬件组成与 10BaseT 相同外,还保持了 10BaseT 的网络拓扑结构,即所有站点都连接到集线器或交换机上,而集线器与站点间的最大距离仍为 100m。由于 100BaseT 对 MAC 子层的接口有所拓展,因此,快速以太网的拓扑结构形式也有相应的发展。

100BaseT 拓扑规则:

(1) 最大 UTP 电缆长度为 100m。

(2) 在一条链路上,对于 I 类中继器(延时为  $0.7\mu\text{s}$  以下),最多只能使用 1 个,可以构成每段长 100m 的两段链路,即站点到中继器距离 100m,中继器到交换机距离 100m。对

于 II 类中继器(延时为  $0.46\mu\text{s}$  以下), 最多使用 2 个, 可有每段长 100m 的两段链路和 5m 长的中继器间链路, 其中站点到第一个中继器(可用集线器)的距离为 100m, 集线器与第二个中继器间距离为 5m, 第二个中继器到路由器或交换机的距离为 100m, 站点到交换机的最大距离为 205m。

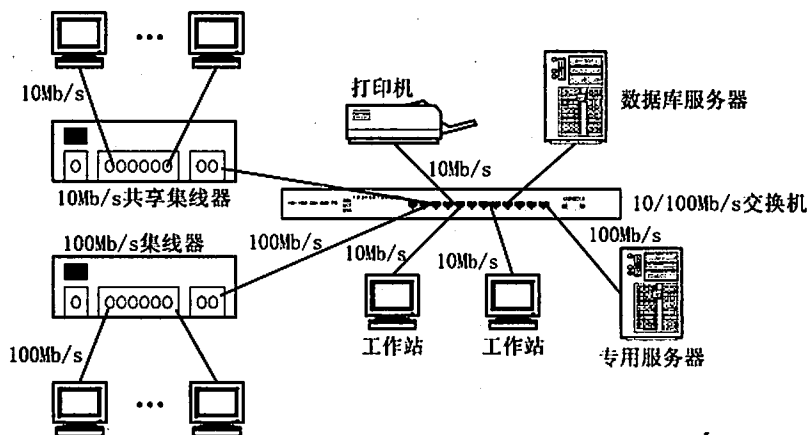


图 1.6 多级交换机快速以太网图

(3) 对于光纤作为垂直布线的拓扑结构, 纵向只能连接一个中继器(Hub), 各站点到 Hub 的最大距离为 100m, 而 Hub 到交换机(或路由器)的垂直向下链路可采用 225m(最大限度)光纤, 站点到交换机的最大距离为 325m。

(4) 利用全双工光纤的拓扑结构, 通过非标准的 100BaseFX 接口连接, 可以使站点(远程)或集线器到路由器或交换机的距离达到 2km。

根据上述规则构成的 100BaseT 拓扑结构如图 1.7 所示。将上述规则进行组合, 利用光纤和交换机、网桥、路由器来连接主干设备、网段和工作站, 可实现大型企业级和政府级网络。

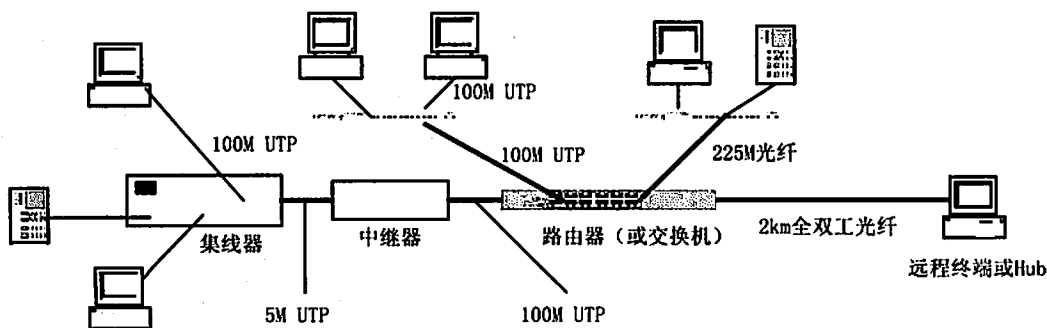


图 1.7 快速以太网的网络拓扑结构图

### 1.2.1.5 千兆位以太网

千兆位以太网是 IEEE 802.3 标准的扩展, 在保持与以太网和快速以太网设备兼容的同时, 提供 1000Mb/s 的数据带宽。千兆位以太网为交换机到交换机和交换机到节点工作站的连接提供了新的全双工操作模式, 还为采用中继器和 CSMA/CD 共享连接提供了半双工操

作模式。千兆位以太网与 IEEE 802.3 网络采用同样的帧格式、大小以及管理方式。它最初要求使用光纤电缆,但目前在 5 类非屏蔽双绞线电缆中也能很好地实现。

### 1. 千兆位以太网的分类

千兆位以太网根据传输介质的不同可以分为以下 4 种,如表 1.1 所示:

表 1.1 千兆位以太网的主要参数

千兆位以太网标准	传输介质	最大传输距离	
		半双工	全双工
1000BaseSX	62.5 $\mu$ m MMF		300m
	50 $\mu$ m MMF	330m	550m
1000BaseLX	MMF	330m	550m
	SMF	330m	5km
1000BaseCX	铜质屏蔽双绞线	25m	25m
1000BaseT	超 5 类非屏蔽双绞线(4 对)	100m	100m

千兆位以太网标准只允许在媒体段中配置一个中继器,实际上在半双工模式下也只能配置一个中继器,增加一个中继器后,铜缆媒体的跨距会增大一倍,而光纤媒体的跨距反而会减少,系统覆盖范围如下:

1000BaseLX/SX: 240m

1000BaseCX: 50m

1000BaseTX: 200m

### 2. 以太网向千兆位以太网的升级方法

现有以太网将逐渐向千兆位以太网升级,升级首先在现有的以太网 LAN 骨干网上进行,然后是服务器连接的升级,最终是工作站的升级。这些升级包括:

(1) 交换机到交换机链路的升级:快速以太网交换机或中继器之间的 100Mb/s 链路会被 1000Mb/s 的链路所替代,以提高骨干网交换机之间的通信速度,并支持更多的交换型和共享型快速以太网网段。

(2) 交换机到服务器链路的升级:在交换机和高性能服务器之间实现 1000Mb/s 链路的连接。并要求服务器安装千兆位以太网网卡。

(3) 快速以太网骨干网的升级:带有 10/100Mb/s 端口的快速以太网交换机可以升级支持多路 100/1000Mb/s 端口的千兆位以太网交换机或路由器和集线器(具有千兆位以太网接口和中继器)。这种升级允许服务器通过千兆位以太网网卡直接连接到骨干网上,可增加用户的高带宽应用与服务器的流量。千兆位以太网可以支持更多的网段、(每个网段更多的)带宽和节点。

(4) 高性能工作站的升级:千兆位以太网网卡可将高性能工作站计算机升级到千兆位以太网。这些工作站计算机要连接到千兆位以太网的交换机或中继器上。

### 3. 千兆位以太网的应用

千兆位以太网可以用于布线间到网络核心的通信,如图 1.8 所示。如需要为个别用户提供 10Mb/s 或 100Mb/s 交换或组交换时,可以通过快速以太网连接,也可以通过千兆位以



太网链路连接。为了提高文件服务器的吞吐性能,它的连接也可以通过千兆位以太网进行。为了提高服务器的吞吐性能,它的连接也可以通过千兆位以太网进行。

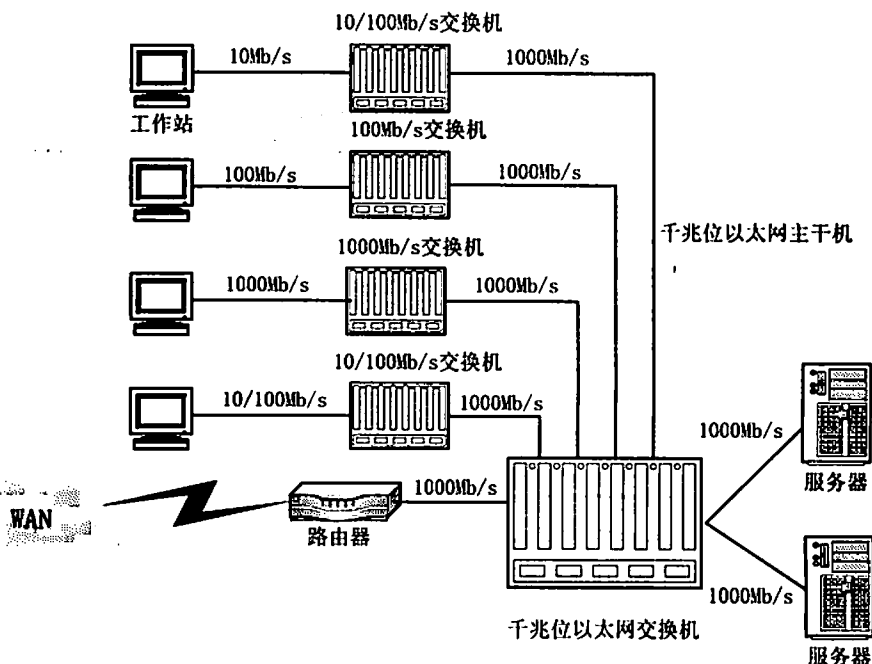


图 1.8 千兆位以太网与多个交换机的连接示意图

### 1.2.1.6 万兆以太网

#### 1. 10GE 以太网

2002 年, IEEE 802.3ae 10Gb/s 以太网标准发布, 以太网的发展势头又得到了一次增强。

物理层: IEEE 802.3ae 大体分为两种类型, 一种是与传统以太网连接, 速率为 10Gb/s 的 LAN PHY, 另一种是连接 SDH/SONET, 速率为 9.58464Gb/s 的 WAN PHY。

传输介质层: IEEE 802.3ae 目前支持 9μm 单模光纤、50μm 多模光纤和 62.5μm 多模光纤。

数据链路层: IEEE 802.3ae 目前继承了 IEEE 802.3 以太网的帧格式和最大/最小帧长度, 支持多层星型连接、点到点连接及其组合, 充分兼容已有应用, 不影响上层应用, 进而降低了升级风险。与传统的以太网不同, IEEE 802.3 仅仅支持全双工方式, 而不支持单工和半双工方式, 不采用 CSMA/CD 机制。IEEE 802.3ae 不支持自协商, 可简化故障定位, 并提供广域网物理层接口。

#### 2. 40GE 以太网

未来两年内, 以太网最高数据传输速率将有望提高至 40Gb/s。Cafiero 称, 业内将 40Gb/s 而非 100Gb/s 确定为以太网下一步发展目标的重要原因在于, 与 100Gb/s 以太网相比, 研发 40Gb/s 以太网在技术上面临的挑战相对较小, 更为切实可行。与此同时, Cafiero 还指出, 实际上, 借助新发布的 Supervisor Engine 720 引擎, Cisco 公司的 Catalyst 6500 旗舰级企业交换平台目前已可以为每一接口卡提供 40Gb/s 的数据传输速率支持。Cafiero 还指出, 新型



以太网技术成功的关键在于能够推动单位数据传输成本的下降。

### 1.2.1.7 局域网交换技术

#### 1. 共享型以太网

所谓共享型以太网即在一个逻辑网络上的每一个工作站都处于一个相同的网段上。以太网采用 CSMA/CD 机制, 整个系统处在一个碰撞域范围中, 系统中每个站点都可能往媒体上发送帧, 那么每个站点要占用媒体的几率就是  $10\text{Mb/s}/n$ , 其中  $n$  为站点数。这种冲突检测方法保证了只能有一个站点在总线上传输。如果有两个站点试图同时访问总线并传输数据, 这就意味着“冲突”发生了, 两站点都将被告知出错。然后它们都被拒发, 并等待一段时间以备重发。

这种机制就如同许多汽车抢过一座窄桥, 当两辆车同时试图上桥时, 就发生了“冲突”, 两辆车都必须退出, 然后再重新开始抢行。当汽车较多时, 这种无序的争抢会极大地降低效率, 造成交通拥堵。

网络也是一样, 当网络上的用户量较少时, 网络上的交通流量较轻, 冲突也就较少发生, 在这种情况下冲突检测法效果较好。当网络上的交通流量增大时, 冲突也增多, 同进网络的吞吐量也将显著下降。在交通流量很大时, 工作站可能会被一而再, 再而三地拒发。

#### 2. 交换型以太网

为了解决共享以太网的问题, 产生了交换型以太网。用交换机代替 Hub, 在交换机上同时存在多个端口间的通道, 就是说系统同时存在多个碰撞域, 每一个碰撞域的一对端口都独占带宽(一个享有发送带宽, 另一个享有接收带宽), 整个系统的带宽与交换机所具有的端口数有关。可以认为, 若每个端口为  $10\text{Mb/s}$ , 则整个系统带宽可达  $10\text{Mb/s} \times n$ , 其中  $n$  为端口数, 若  $n=10$ , 则系统带宽可达  $100\text{Mb/s}$ 。

#### 3. 全双工以太网

传统的共享型以太网只以半双工模式工作, 即网络在同一时间要么发送数据, 要么接收数据, 而不能同时发送数据和接收数据。全双工以太网与传统半双工以太网技术之间区别在于: 每个端口和交换机背板之间都存在两条逻辑通道。这样, 每一个端口就可以同时接收和发送帧, 不再受到 CSMA/CD 的约束, 在端口发送帧时不再发生帧的碰撞, 已无碰撞域的存在。这样一来, 端口之间媒体的长度仅仅受到数字信号在媒体上传输衰变的影响, 而不像传统以太网半双工传输时还要受到碰撞域的约束。其优点是, 传输速度加快, 对于光纤传输介质, 传输距离变长。

### 1.2.1.8 局域网设备

计算机网络的组成可分为硬件与软件两大部分, 硬件部分包括文件服务器、工作站、网卡、传输媒介、接头、网络中的设备、不间断电源系统(UPS)、打印机等、软件部分则包括网络操作系统(如 Windows NT、Linux、Novell、Netware 等)、网络管理系统和应用软件系统。

#### 1. 服务器与工作站

服务器的主要功能是通过网络操作系统控制和协调网络各工作站的运行, 处理和响应各工作站同时发送来的各种网络操作要求, 提供网络服务。工作站是网络各用户的工作场

所,通常是一台微机或终端。

根据应用类型网络服务器可分为:文件服务器、应用程序服务器、通信服务器等几大类。通常一个网络至少有一个文件服务器,网络操作系统及其实用程序和共享硬件资源都安装在文件服务器上。

按照网络服务器的设计思想分类,一般把服务器分成3种类型,一种是入门级服务器,有时也称为PC服务器;一种是工作组级服务器,在中小企业的业务部门里使用,有时也称为部门级或工作组级服务器。还有一种企业级服务器,一般担当企业的整体网络部署。

## 2. 网卡

网卡(Network Interface Card, NIC)也叫网络适配器,是连接计算机与网络的硬件设备。网卡插在计算机或服务器的扩展槽中,通过网线(如双绞线、同轴电缆或光纤)与网络交换数据、共享资源。在网络中,网卡的任务是双重的:一方面它负责接收网络上传过来的数据包,解包后,将数据通过主板上的总线传输给本地计算机;另一方面它将本地计算机上的数据打包后送入网络。

## 3. 传输介质

### (1) 同轴电缆

同轴电缆抗干扰性好、频带较宽、数据传输稳定、价格适中、性价比高。同轴电缆中央是一根内导体铜质芯线,外面依次包有绝缘层、网状编织的外导体屏蔽层和塑料保护外层。

通常按特性阻抗数值的不同,可将同轴电缆分为 $50\Omega$ 基带同轴电缆和 $75\Omega$ 宽带同轴电缆。前者用于传输基带数字信号,是早期局域网的主要传输媒体;后者是有线电视系统CATV中的标准传输电缆,在这种电缆上传输的信号采用了频分复用的宽带模拟信号。

$50\Omega$ 基带同轴电缆可分为两类:粗缆和细缆。粗缆用于10Base5以太网,最大干线段长度为500m,最大网络干线电缆长度为2500m,每条干线段支持的最大节点数100个,收发器之间的最小距离1.5m,收发器电缆的最大长度为50m;细缆用于10Base2以太网,最大干线段长度为185m,最大网络干线电缆长度为925m,每条干线段支持的最大节点数30个,BNC-T型连接器之间的最小距离0.5m。使用基带同轴电缆组网,需要在两端连接 $50\Omega$ 的反射电阻,又叫终端匹配器。

### (2) 双绞线

双绞线是由两条导线按一定扭矩相互绞合在一起的类似于电话线的传输媒体,每根线加绝缘层并用颜色来标记。成对线的扭绞旨在使电磁辐射和外部电磁干扰减到最小。使用双绞线组网,双绞线与网卡、双绞线与集线器的接口叫RJ-45,俗称水晶头。

双绞线分为屏蔽双绞线(STP)和非屏蔽双绞线(UTP),STP双绞线内部包了一层皱纹状的屏蔽金属物质,并且多了一条接地用的金属铜丝线,因此它的抗干扰性比UTP双绞线强,阻抗值通常为 $150\Omega$ 。对于UTP双绞线,阻抗值通常为 $100\Omega$ ,每条双绞线最大传输距离为100米。

双绞线的制作有两种方法:一是直通线,即双绞线的两个接头都按568B线序标准连接;二是交叉线,即双绞线的一个接头按EIA/TIA 568A线序连接,另一接头按EIA/TIA 568B线序连接。



### (3) 光纤

光纤是新一代的传输介质,与铜质介质相比,光纤具有一些明显的优势。因为光纤不会向外界辐射电子信号,所以使用光纤介质的网络无论是在安全性、可靠性还是在传输速率等网络性能方面都有了很大的提高。

根据光在光纤中的传输方式,可将光纤分为两种类型:多模光纤和单模光纤。

### (4) 无线传输

无线传输主要分为无线电、微波、红外线及可见光几个波段。

无线电微波通信在数据通信中占有重要地位。微波的频率范围 300MHz~300GHz,但主要使用 2GHz~40GHz 的频率范围。微波通信主要有两种方式:即地面微波接力通信和卫星通信。

## 4. 网络互连设备

常用网络互连设备有中继器、集线器、网桥、交换机、路由器以及网关等。

### (1) 中继器(Repeater)

中继器是网络物理层的一种介质连接设备,它工作在 ISO/OSI 参考模型的第一层(物理层)。当局域网物理距离超过了允许的范围时,可用中继器将该局域网的范围进行延伸。

### (2) 集线器(Hub)

集线器从工作原理上看就是一个多端口中继器,它起到一个信号分散器的作用,它也在 ISO/OSI 参考模型的第一层(物理层),它通过一个端口接收信号然后再发送到其他所有端口。它是在局域网上广泛被使用的网络设备,可以用来将若干台计算机通过双绞线或同轴电缆连到集线器,从而构建一个局域网。

### (3) 网桥(Bridge)

网桥工作在 ISO/OSI 参考模型的第二层(数据链路层),与高层协议无关,因此只能连接具有相同高层协议的网络。网桥的工作原理是,通过数据链路层的逻辑链路控制子层选择子网路径,接收完整的 MAC 的数据帧并进行差错校验,再根据 MAC 中的源或目的地址决定帧的去向。如果是传给本网段的某一站点,则不予转发,如果目的地址是其他网络段的,则在它连接的所有网络段转发该 MAC 帧。在转发该帧之前,网桥对帧的内容和格式不作修改或仅作少量的修改后发送到物理层,再由物理层传输介质发送到另外一个子网。

数据链路层连接两个局域网络段指的是网间通信从网桥传送,网内通信被网桥隔离。当网络负载重而导致性能下降时,用网桥可将其分为两个或多个网络段,从而最大限度地缓解网络通信繁忙的程度,提高通信效率。

### (4) 交换机(Switch)

集线器(Hub)虽然有多个端口,但同一时间只允许一个端口发送或接收数据;而交换机则是采用程控交换机的原理设计的。交换机允许多对端口同时发送或接收数据,每一个端口独占整个带宽,从而提供了一种提高数据传输速率的方法,交换机能够将以以太网的速率提高至真正的 10Mb/s 或 100Mb/s。交换机工作在 ISO/OSI 参考模型的第二层(数据链路层),目前局域网内广泛采用交换机设备。

### (5) 路由器(Router)

当两个不同类型的网络彼此相连时,必须使用路由器。路由器工作在 ISO/OSI 参考模型的第三层(网络层),能够提供路由选择、流量控制、协议转换、分组过滤、子网分割等

功能。可广泛应用于局域网之间、局域网与广域网之间以及广域网之间的互联。路由器的互连能力强,可以执行复杂的路由选择算法,处理的信息量比网桥多,但处理速度比网桥慢。

路由器在局域网系统中的应用:

- 局域网互联:连接多个局域网系统并实现局域网系统之间的数据转发。
- 局域网隔离:连接多个局域网系统并实现局域网系统之间的数据隔离。
- 局域网与广域网互连:局域网通过路由器连接广域网,实现对远程主机的访问。

#### (6) 网关(Gateway)

当连接两个结构完全不同的网络时,必须使用网关。网关又称协议变换器,它工作于传输层及其以上的层次,用于在不同网络之间实现协议转换的专用网络通信设备。

网关可以设在服务器、微型机或大型机上。常见的网关有:

- ① 电子邮件网关:可以从一种类型的系统向另一种类型的系统传输数据。
- ② IBM 主机网关:可以在一台个人计算机与 IBM 大型机之间建立和管理通信。
- ③ 互联网网关:允许并管理局域网和互联网间的接入,可以限制某些局域网用户访问互联网,反之亦然。
- ④ 局域网网关:可以使运行于 OSI 模型不同层上的局域网网段间相互通信。路由器甚至只用一台服务器就可以充当局域网网关。局域网网关也包括远程访问服务器。它允许远程用户通过拨号方式接入局域网。

#### 1.2.1.9 计算机网络接入技术

终端远程接入局域网、局域网与局域网远程互联或局域网接入广域网,必须借助公共传输网络。

公共传输网络的接入技术主要有:公共交换电话网 PSTN、综合业务数字网 ISDN、X.25 分组交换网、数字数据网 DDN、帧中继 FR、异步传输模式 ATM、数字用户线路 xDSL、宽带接入、HFC 和 Cable Modem 接入技术等。

##### 1. PSTN 接入技术

所谓“拨号接入”,就是指通过普通电话线利用 Modem(Modulator Demodulator, 调制解调器)使用 PSTN(Public Switched Telephone Network, 公用交换式电话网)来传输数据,普通拨号 Modem 的最高速率为 56Kb/s。其需要的接入硬件需要具备一台调制解调器,一条电话线、集线器或交换机、代理服务器(网卡和 Modem 的连接端口)等。代理服务器可安装 WinGate、Sygate 等代理软件,以便代理局域网内的其他计算机访问 Internet。其拓扑图如图 1.9 所示,代理服务器的串行口 Com 通过串行线与 Modem 相连,网卡通过双绞线与交换机或集线器相连,并根据需求设置该网卡的 IP 地址(私有地址),如 192.168.1.1,子网掩码为 255.255.255.0,局域网内其他计算机设置的 IP 地址与该服务器的网卡地址位于同一个网段内。

也可使用带有 PSTN 端口的路由器接入 Internet。其拓扑图如图 1.10 所示。

##### 2. ISDN 接入技术

ISDN 是 Integrated Services Digital Network(综合业务数字网)的缩写,能在一根普通电话线上提供语音、数据、图像等综合性业务。ISDN 在一对普通的电话用户线路上,提供 2 个双向的 64Kb/s 的 B 通道和一个 16Kb/s 的 D 通道。B 通道是承载通道,可以传送语音和



数据、两个 B 通道既可以单独使用,也可以捆绑起来传送数据,可达到 128Kb/s 的速率。ISDN 可连接 8 台终端或电话,有 2 台终端(例如:一部电话、一台计算机或一台数据终端)可以同时使用。对于用户而言,同样的一对普通电话线原来只能接一部电话机,而申请了 ISDN 后,通过一个称为 NT 的转换盒,就可以同时使用数个终端。在一根普通电话线上,可以提供以 64Kb/s 速率为基础并可达到 128Kb/s 的上网速度的数字连接。

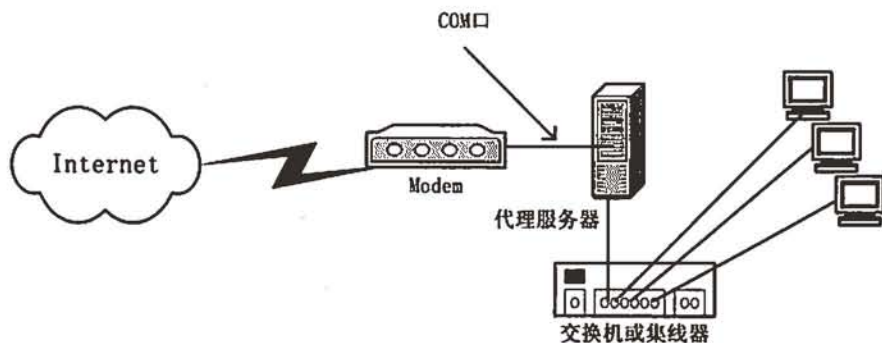


图 1.9 用调制解调器连接 Internet

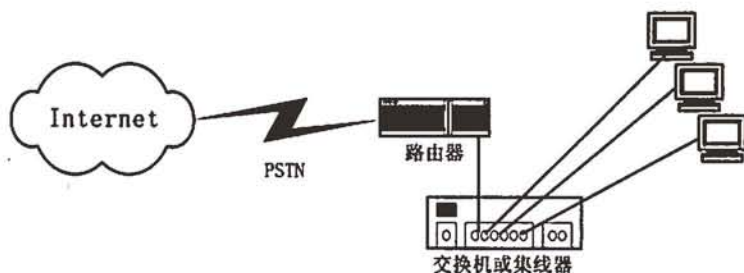


图 1.10 用路由器接入 Internet

局域网用户可通过 ISDN 专线接入 Internet,其拓扑结构如图 1.11 所示。所需的硬件设备有 NT1、ISDN 专线、交换机或集线器、代理服务器(ISDN 卡和网卡)等。代理服务器可安装 WinGate、Sygate 等代理软件,以便代理局域网内的其他计算机访问 Internet。

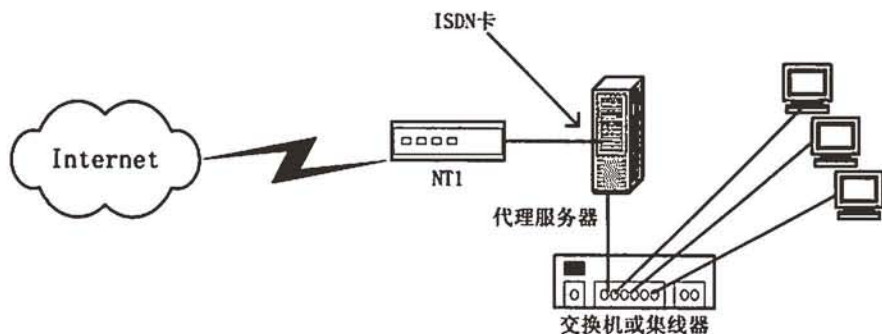


图 1.11 局域网使用 ISDN 专线接入 Internet

也可采用 ISDN 路由器接入 Internet,其拓扑图如图 1.12 所示。

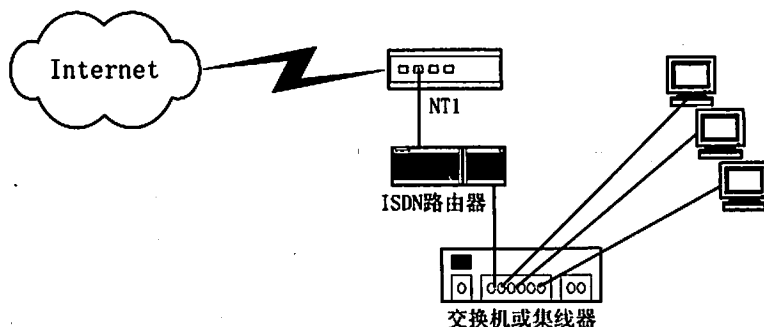


图 1.12 局域网使用 ISDN 路由器接入 Internet

### 3. ADSL 接入技术

ADSL 是英文 Asymmetrical Digital Subscriber Loop(非对称数字用户环路)的缩写, ADSL 技术是运行在原有普通电话线上的一种新的高速宽带技术, 它利用现有的一对电话铜线, 为用户提供上、下行非对称的传输速率(带宽)。非对称主要体现在上行速率(最高 640Kb/s)和下行速率(最高 8Mb/s)的非对称性上。上行(从用户到网络)为低速的传输, 可达 640Kb/s; 下行(从网络到用户)为高速传输, 可达 8Mb/s。在不影响原有语音信号的基础上, 扩展了已有电话线路的功能。

局域网用户可通过 ADSL 接入 Internet, 其拓扑图如图 1.13 所示。所需的硬件设备有语音/数据分离器、ADSL 专线、交换机或集线器、代理服务器(两块网卡)等。代理服务器上连接 ADSL Modem 的那一块网卡设置电信公司提供的 IP 地址、子网掩码、DNS、网关等参数, 内网可设置私有地址, 并安装代理服务软件, 以便代理局域网内的其他计算机访问 Internet。

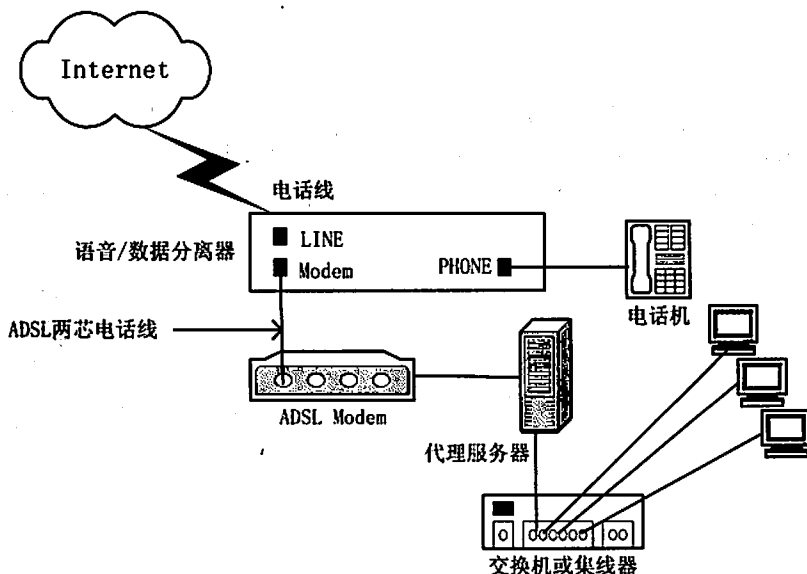


图 1.13 局域网用户使用 ADSL 接入 Internet

也可利用 ADSL 路由器接入 Internet, 其拓扑图如图 1.14 所示。

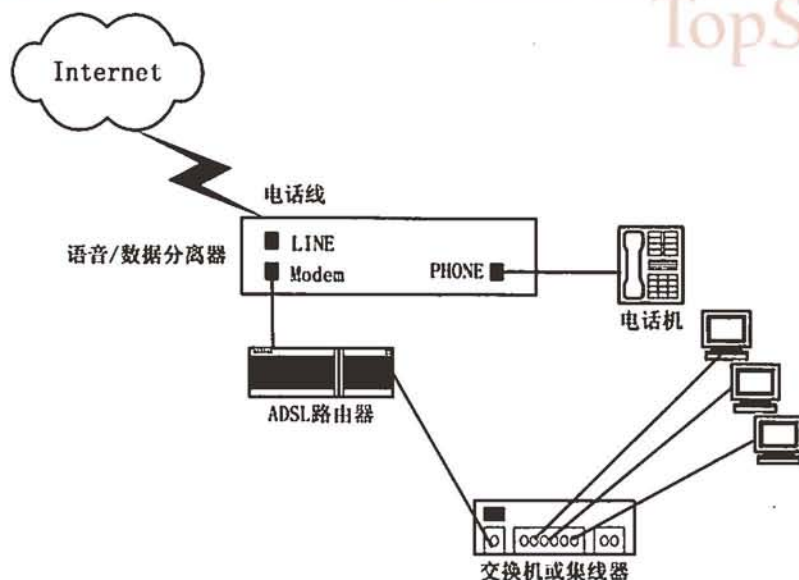


图 1.14 局域网使用 ADSL 路由器接入 Internet

#### 4. 宽带 IP 接入技术

宽带 IP 网以光纤通信为基础，以成熟的 IP 技术为核心，采用路由器和交换机等设备组网，可为用户提供 10M/100M/1000M 可选接入速率，其速率是目前电话拨号上网的 170 多倍。

宽带 IP 网的建设目标是铺设光纤到小区、到大楼，最终以光纤到户为目标。目前一般采用光纤加局域网的方式实现群体用户接入宽带网络。其拓扑图如图 1.15 所示。

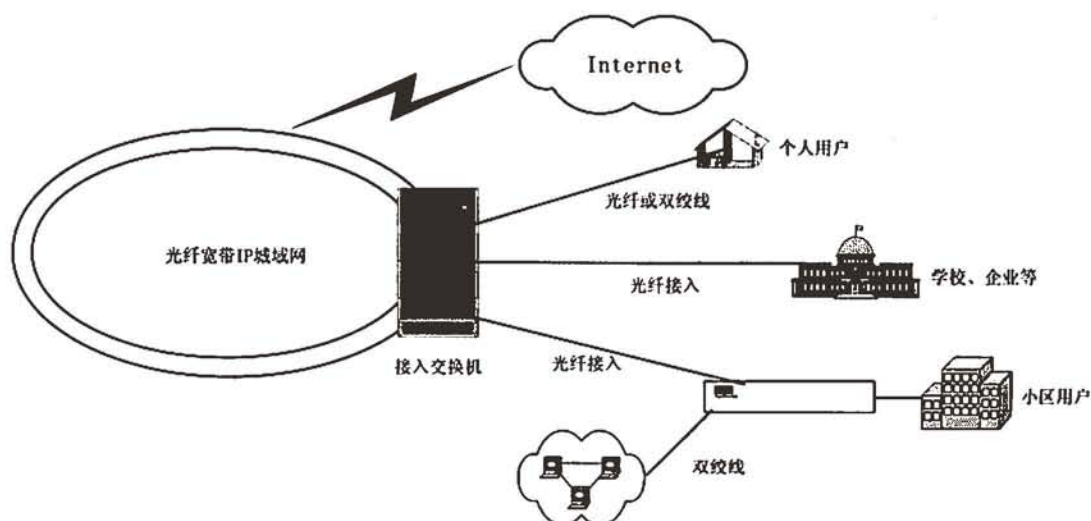


图 1.15 局域网宽带 IP 接入 Internet

#### 5. HFC 和 Cable Modem

HFC 网是指光纤同轴电缆混合网，它是一种新型的宽带网络，采用光纤到服务区，而在进入用户的“最后 1 千米”采用同轴电缆，最常见的是有线电视网络。HFC 网络大部分

采用传统的高速局域网技术,而 Cable Modem 是最重要的组成部分。

Cable Modem 可以翻译成电缆调制解调器或线缆调制解调器,它是一种将数据终端设备连接到有线电视网(CATV),以使用户能够进行数据通信访问 Internet 等信息资源的设备。

#### 6. 数据通信网接入技术

局域网用户还可以通过 DDN 网、X.25 网、帧中继网、ATM 网接入 Internet,其核心设备是路由器等网络终端接入设备。其拓扑结构如图 1.16 所示。

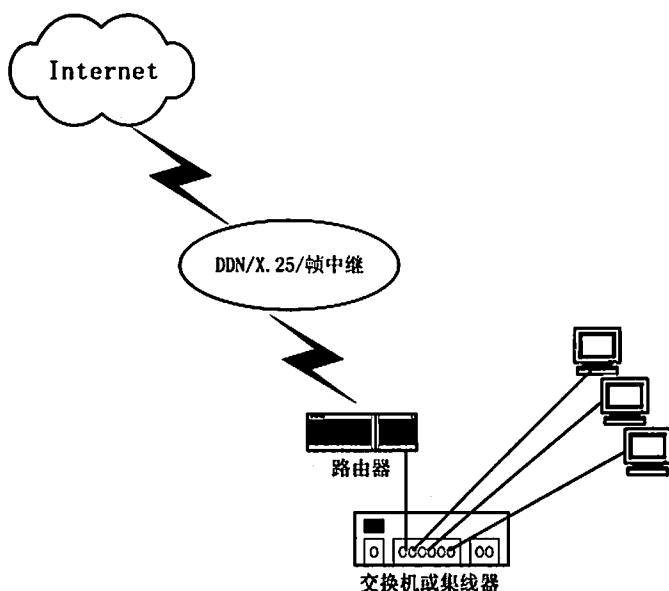


图 1.16 局域网使用数据通信网接入 Internet

##### (1) X.25 分组交换网

X.25 是 CCITT 制定的在公用数据网上供分组型终端使用的,数据终端设备(DTE)与数据通信设备(DCE)之间的接口建议。它只是一个经由虚电路服务为基础的对公用分组交换网接口的规格说明。它动态地对用户传输的信息流分配带宽,能够有效地解决突发性、大信息流的传输问题,分组交换网络同时可以对传输的信息进行加密有有效的差错控制。

X.25 一般只用于要求传输费用少,而远程传输速率要求又不高的广域网使用环境。速率为 9600b/s~64Kb/s。

##### (2) 数字数据网(DDN)

DDN 是利用数字通道提供半永久性连接电路,向用户提供端到端的中高速率、高质量的数字专用电路,全程实现数字信号透明传输的数据传输网。DDN 网通常由 4 部分组成,即包括本地传输系统、复用与交叉连接系统、局间传输与同步系统和网络管理系统等。DDN 干线主要采用光缆、数字微波与卫星信道,所提供的信道是非交换型的半永久电路,其中通常由电信部门在用户申请时设定,修改并非经常性的。

DDN 采用脉冲编码调制(PCM)的数字中继方式,传输距离远,具有传输速度快、质量好、性能稳定和带宽利用率高等优点。速率可达 2Mb/s。

##### (3) 帧中继

帧中继是为了克服 X.25 的缺点,提高性能而发展起来的一种高速分组交换与传输技



术。帧中继是一种减少节点处理时间的技术。帧中继认为帧的传送基本上不会出错,因此每个节点只要一知道帧的目的地址,就立即转发,大大减少了帧在每一个节点的时延,比传统的 X.25 的处理时间少一个数量级。

帧中继的设计目标主要是针对局域网之间的互联,它以面向连接的方式,合理的数据传输率和低廉的价格提供数据通信服务。帧中继的主要思想是“虚拟租用线路”。帧中继采用帧作为数据传送单元,网络的带宽根据用户帧传输的需要,可以采用统计复用的方式动态分配,可以充分复用网络资源,提高了中继带宽的利用率,尤其对突发信息的适应性比较强。帧中继用户的接入速率在 64Kb/s~2Mb/s。

#### (4) 异步传输模式(ATM)

ATM 是 Asynchronous Time division multiplexing 的缩写,译为“异步传输模式”,它是高速分组传送模式为主,综合电路传输模式优点的一种宽带传输模式。

ATM 系统是使用异步时分复用技术的快速分组交换方式,它将信息流分割成固定长度的 ATM 信元,能比较容易地实现各种信息流混合在一起的多媒体通信,能根据业务类型、传输速率等要求动态分配有效容量,对高速信息元传输频次高,对低速信息元传输频次低。因此 ATM 能采用单一的交换方式,支持从窄带语音、数据传输到 HDTV 等范围极广的各种业务。

ATM 信元是固定长度的分组,并使用空闲信元来填充信道,从而使信道被分为等长的时间小段。每个信元共有 53 个字节,分为 2 个部分。前面 5 个字节为信头,主要完成寻址的功能;后面的 48 个字节为信息段,用来装载来自不同用户,不同业务的信息。ATM 接入的速率可达 155Mb/s~622Mb/s。

### 1.2.2 典型例题分析

**例 1** 目前局域网广泛采用以太网技术。局域网互联时,通常采用中继器、集线器、网桥、交换机、路由器、网关等设备,请简要回答下列问题。

**【问题 1】**以太网的标准是什么?

**【问题 2】**中继器、集线器、网桥、交换机、路由器、网关分别工作在 ISO/OSI 参考模型的哪一层?

**【问题 3】**简述路由器的特点?

**分析:**问题 1 是考查以太网的概念,要求考生对以太网的标准有所了解,属于识记层次,较容易。

问题 2 是考查局域网互联设备工作在 ISO/OSI 参考模型的哪一层。中继器是网络物理层的一种介质连接设备,它工作在 ISO/OSI 参考模型的第一层(物理层)。当局域网物理距离超过了允许的范围时,可用中继器将该局域网的范围进行延伸。集线器从工作原理上看就是一个多端口中继器,它起到一个信号分散器的作用,它也工作在 ISO/OSI 参考模型的第一层(物理层),它通过一个端口接收信号然后再发送到其他所有端口。网桥工作在 ISO/OSI 参考模型的第二层(数据链路层),负责接收和转发数据帧,并对数据帧进行管理。交换机从工作原理上看就是一个多端口网桥,它利用存储转发和过滤技术来分割网段,使局域网整体带宽得到成倍提高。路由器工作在 ISO/OSI 参考模型的第三层(网络层),它能够在复杂网络中为网络数据的传输自动进行路径选择。网关工作在 ISO/OSI 参考模型的传

输层及其以上的层次,用于在不同网络之间实现协议转换的专用网络通信设备。

问题3考查路由器的特点。

答案:

【问题1】以太网的标准是 IEEE 802.3。

【问题2】中继器工作在 ISO/OSI 参考模型的第一层、集线器工作在 ISO/OSI 参考模型的第一层、网桥工作在 ISO/OSI 参考模型的第二层、交换机工作在 ISO/OSI 参考模型的第二层、路由器工作在 ISO/OSI 参考模型的第三层、网关工作 ISO/OSI 参考模型的传输层及其以上的层次。

【问题3】路由器的特点如下:

(1) 更强的异种网络互联能力。路由器不仅能实现不同类型的局域网互联,而且可以用于局域网与广域网、广域网与广域网的互联,同时,它还提供不同网络地址格式的转换功能。

(2) 有较好的拥挤控制能力。路由器具有各种解决拥挤的方法,而网桥只能通过加大缓存来局部解决拥挤问题。同时,路由器可以隔离广播信息,避免出现广播风暴。

(3) 具有防火墙功能。路由器通常有多种隔离信息包的方法,从而进一步加强网络的安全保密性,防止网络系统和系统内的数据遭到攻击和破坏。

(4) 便于网络管理和维护。路由器连接的各个网络仍是独立的子网,便于各自管理和维护。并且,通过路由器提供的网管功能,可以随时对各子网的工作状况进行监视和控制,及时发现和解决可能出现的问题。

例2 阅读以下说明,回答问题。

【说明】图 1.17 是某办公局域网的结构图,采用 8 口 Hub 将客户机、打印机及服务器相联,形成一个小型的办公网络。

【问题1】该网络采用的媒体访问控制技术是什么?

【问题2】局域网的主要网络拓扑有哪些?图 1.17 的采用了哪种网络拓扑?

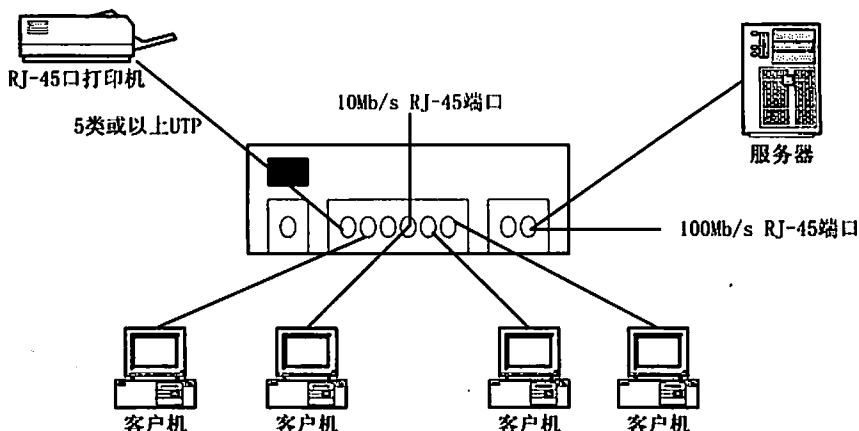


图 1.17 办公局域网拓扑图

【问题3】Hub 与服务器、客户机之间采用什么传输介质。

分析: 问题1考查共享型以太网的概念,用 Hub 组建的以太网为共享型以太网,采用



CSMA/CD 媒体访问控制技术是共享型以太网特征。

问题2 考查局域网的拓扑结构分类。局域网的拓扑结构通常分为三种，分别是总线型拓扑结构、星型拓扑结构和环型拓扑结构。

总线型结构是使用同一媒体或电缆连接所有端用户的一种方式，也就是说，连接端用户的物理媒体由所有设备共享。

星型结构存在着中心节点，每个节点通过点对点的方式与中心节点相连，任何两个节点之间的通信都要通过中的节点来转接。

环型结构在 LAN 中使用较多。这种结构的传输媒体从一个端用户到另一个端用户，直到将所有端用户连成环型。

问题3 是考查局域网采用的传输媒体，在 Hub 组建的以太网中，采用两端都装有同样的 RJ-45 型接头(水晶头)，每一个工作节点都需要一根双绞线电缆，用来连接工作节点上的网卡与集线器。

答案：

【问题1】CSMA/CD

【问题2】局域网在网络拓扑上主要采用了环型、星型和总线型结构。图 1.17 中采用的是星型拓扑结构。

【问题3】双绞线

例3 对于普通的 10M Hub，若连接 10 个设备，则每个设备的速率是 (1)，Hub 的带宽为 (2)；对于 10M Switch，若连接 10 个设备，则每个设备的速率是 (3)，交换机的带宽是 (4)。

分析：一台 10 口的 10BaseT 集线器，每个端口所分配的带宽为  $10\text{Mb/s}/10=1\text{Mb/s}$ ；如果是一台 10 口的 10Base 交换机，同一时刻可有 5 个交换通路存在，也就是说可以有 5 个 10Mb/s 的信道，有 5 对端口进行数据传输，5 个端口分别发送 10Mb/s 的数据，另外 5 个端口分别接收 10Mb/s 的数据。这样每个端口所分配到的带宽为 10Mb/s，在理想的负荷状态下，整个交换机的带宽为  $10\text{Mb/s} \times 10 = 100\text{Mb/s}$ 。

答案：(1)1Mb/s (2)10Mb/s (3)10Mb/s (4)100Mb/s

例4 假设光速  $C=3 \times 10^8\text{m/s}$ ，物理层延迟  $t_{\text{PHY}}=0.15 \times 10^{-5}\text{s}$ ，电信号在电缆中的传播速度为  $0.7C$ ，最小帧长  $L_{\text{min}}=512$  字节。在无中继器和集线器的情况下，请计算快速以太网网络系统跨距的近似值。

分析：在 CSMA/CD 技术中，碰撞槽时间用来表征数据帧发送过程中发生碰撞时间的上限，即在碰撞时间内可能会检测到碰撞，而一过这段时间，就不可能检测到碰撞，数据帧发送成功。碰撞槽时间与共享媒体最大跨距  $S$  和物理层延迟  $t_{\text{PHY}}$ ，其近似计算公式为：

$$\text{slot time} \approx 2S/0.7C + 2t_{\text{PHY}}$$

为了能在数据帧发送期间检测到碰撞，数据帧发送时间至少应为碰撞槽时间，即  $\text{slot time} = L_{\text{min}}/R$ ，( $L_{\text{min}}$  称为最小帧长度， $R$  为传输速率，在 10Mb/s 以太网环境中， $R=10 \times 10^6\text{b/s}$ ，在 100Mb/s 以太网环境中， $R=100 \times 10^6\text{b/s}$ ) 则系统跨距  $S$  的表达式为：

$$S \approx 0.35C \times (L_{\text{min}}/R - 2t_{\text{PHY}})$$

答案:  $\text{slot time} \approx 2S/0.7C + 2t_{\text{PHY}}$

$$L_{\min}/R = \text{slot time}$$

$$S \approx 0.35C \times (L_{\min}/R - 2t_{\text{PHY}})$$

$$\approx 0.35 \times 3 \times 10^8 \times (512/10^8 - 2 \times 0.15 \times 10^{-5})$$

$$\approx 222.6(\text{m})$$

所以网络系统跨距约为 222.6 米。

例 5 简要回答有关局域网传输媒体的问题。

【问题 1】局域网的传输媒体包括哪些种类?

【问题 2】目前局域网上常用哪几种传输媒体?

【问题 3】目前局域网上能达到最高传输率的传输媒体是哪一种?

【问题 4】要获得最佳的数据传输安全保密性的传输媒体是哪一种?

分析: 局域网的传输媒体主要有: 双绞线、同轴电缆、光缆、无线传输四大类。最常用的是双绞线和光缆, 这与它们各自的特点是分不开的。一般短距离采用双绞线, 长距离则使用光缆。

光纤利用全内反射来传输经信号编码的光束。能够实现最高速率的传输。所以说目前局域网能达到最高传输率的传输媒体是光缆。

光纤不受电磁干扰或噪声的影响, 这种特性允许在很长的距离内进行高速数据传输, 并能提供优良的安全保密性, 所以说要想获得最佳的数据传输安全保密性, 就要采用光缆作为这种传输媒体。

答案:

【问题 1】传输媒体是收发双方之间进行通信的物理信号通路。用于局域网的传输媒体有双绞线、同轴电缆、光缆和无线传输媒体四类。

【问题 2】目前局域网常用传输媒体为双绞线和光缆。

【问题 3】目前局域网上能达到最高传输率的传输媒体是光缆。

【问题 4】要获得最佳的数据传输安全保密性的传输媒体是光缆。

例 6 阅读以下说明, 回答问题。

【说明】某大型企业包括网络中心、管理部、生产部、市场部、财务部、人事部等部门, 各部门内部都已经建设了自己的局域网系统。现要将企业内部各部门的局域网互联起来。建设企业内联网。

组网要求: 能够实现企业内部各部门局域网系统的有效隔离, 防止跨部门的非法访问; 各部门之间根据需要可以有效互连通信, 将信息由部门级共享提高企业级共享; 各部门的计算机都可以连接访问 Internet。

【问题 1】请简述其实施方案并画出网络拓扑结构示意图。

【问题 2】简述路由器在局域网组网工程中的应用。

分析: 根据用户需求可以总结出用户对现有局域网系统的三点要求: 局域网隔离、局域网互联以及局域网与广域网互联。这恰好就是路由器在局域网系统中的三项应用。因此可以在组网方案中应用路由器作为网络互联设备。



答案:

【问题 1】各部门局域网之间通过路由器互联起来,通过配置路由器实现各部门之间的访问控制策略;路由器具有连接 Internet 的广域网端口,企业内部各部门局域网系统中的计算机可以通过路由器访问 Internet,其拓扑图如图 1.18 所示。

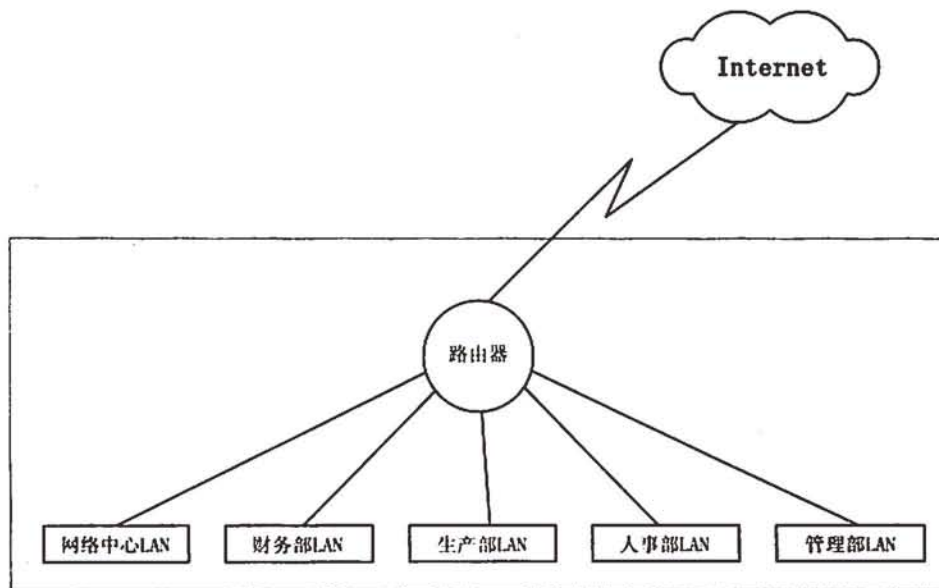


图 1.18 某企业内部网组网拓扑图

【问题 2】路由器在局域网系统中的应用主要有:

- (1) 局域网互联:连接多个局域网系统并实现局域网系统之间的数据转发。互联的局域网系统可以是相同类型,也可以是不同类型。
- (2) 局域网隔离:连接多个局域网系统并实现局域网系统之间的数据隔离。
- (3) 局域网与广域网互联:局域网通过路由器连接广域网,实现对远程主机的访问。

例 7 阅读以下的说明,回答问题。

【说明】某单位的办公室中要组建一个小局域网,其中有 PC 机 4 台、服务器 1 台、打印机 1 台,现拟采用 10/100Mb/s 交换机组建该单位网络。

【问题 1】请列出需要准备的网络设备及配件。

【问题 2】画出网络拓扑结构图,并注明网络设备和传输媒体的名称、规格(速率、端口数)

分析:由于网络服务器和网络的传输数据量大、工作频繁,因此网络交换机和网络服务器之间的传输线路成为网络传输性能的瓶颈,是设计时应考虑的重点因素,因此,可以选择带有 1~2 个 100Mb/s 端口的交换机,并将网络服务器联入高速端口。对于网络传输速率要求不高的普通客户机,则可以接入 10Mb/s 端口。

答案:

【问题 1】需要准备的网络设备及配件有带有 1~2 个 100Mb/s 端口的交换机;服务器购置 100Mb/s 网卡,客户机可购置 10Mb/s 网卡;准备两端带有 RJ-45 型接头的 5 类非屏蔽

直通双绞线。

【问题 2】选择 8 口交换机(带有两个 100Mb/s 端口), 网络拓扑结构图如图 1.19 所示。

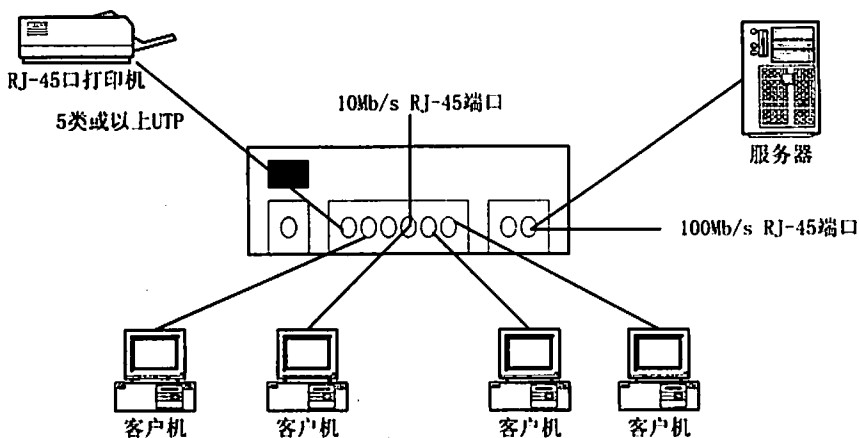


图 1.19 办公室局域网组网拓扑结构图

例 8 阅读以下说明, 回答问题。

【说明】某学校拟组建一个小型校园网, 拓扑图如图 1.20 所示。具体设计如下:

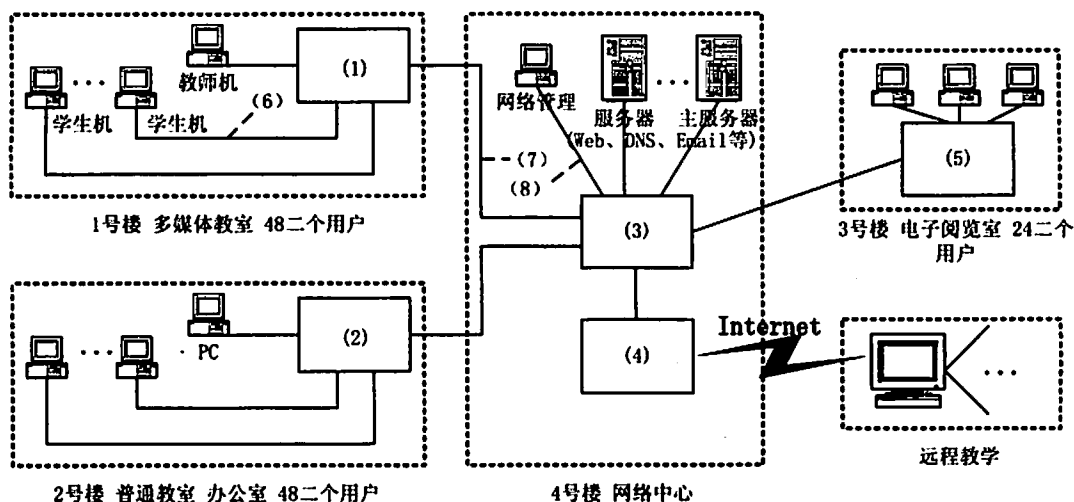


图 1.20 某学校局域网拓扑结构图

### (1) 设计要求

终端用户包括: 48 个校园网普通用户; 一个有 24 个多媒体用户的电子阅览室; 一个有 48 个用户的多媒体教室(性能要求高于电子阅览室)。

服务器提供 Web、DNS、E-mail 服务。

支持远程教学, 可以接入互联网, 具有广域网访问的安全机制和网络管理功能。

各楼之间的距离为 500 米。

### (2) 可选设备

可选设备如表 1.2 所示。

表 1.2 可选设备清单

设备名称	数量(台)	特 性
交换机 Switch1	1	具有两个 100BaseTX 端口和 24 个 10BaseT 端口
交换机 Switch2	2	各具有两个 100M 快速以太网端口(其中一个 100BaseTX、一个 100BaseFX)和 24 个 10BaseT 端口
交换机 Switch3	2	各配置 2 端口 100BaseFX 模块、24 个 100BaseTX 快速以太网端口
交换机 Switch4	1	配置 4 端口 100BaseFX 模块、24 个 100BaseTX 快速以太网端口。
路由器 Router1	1	提供了对内的 10/100M 局域网接口, 对外的 128K 的 ISDN 或专线连接, 同时具有防火墙功能。

## (3) 可选介质

3 类双绞线、5 类双绞线、多模光纤。

【问题 1】依据给出的可选设备进行选型, 填写(1)~(5)处空缺的设备名称 (每处可选一台或多台设备)。

【问题 2】填写(6)~(8)处空缺的介质(所给介质可重复选择)。

分析: 该网络采用快速以太网技术, 各楼层主干之间采用光纤通过 100BaseFX 模块或 5 类双绞线 100BaseTX 端口与中心交换机相连, 楼层内交换机采用级联的方式相连, 通过路由器将网络中心交换机与 Internet 相连。客户端机器通过 5 类双绞线与交换机 10 或 100Mb/s RJ-45 端口相连。由于 Web、DNS、E-mail 服务器访问量较大, 采用 100Mb/s RJ-45 端口与服务器相连。

答案:

【问题 1】

- (1) 两台交换机 Switch3。
- (2) 一台交换机 Switch1 和一台交换机 Switch2。
- (3) 一台交换机 Switch4。
- (4) 一台路由器 Router1。
- (5) 一台交换机 Switch2。

【问题 2】

- (6) 5 类双绞线
- (7) 多模光纤
- (8) 5 类双绞线

例 9 某实验室原有 10BaseT(8 口 Hub)以太网, 现增加一台服务器、10 台客户机, 拟采用 10/100Mb/s 交换机对网络进行扩建, 同时要求保护和兼顾原有的投资。请画出网络拓扑结构图, 并注明网络设备和传输媒体的名称、规格 (速率、端口数)。

分析: 选择一台 10/100Mb/s 交换机:

(1) 为保证服务器的 100Mb/s 传输速率的需求, 将有高传输速率要求的服务器接入交换机的 100Mb/s 专用端口。

(2) 使用交换机上的 10Mb/s 端口连接共享集线器, 从而保留了原有 10BaseT 网络上

的所有低速节点和设备。

(3) 尽可能多地将一些有固定带宽要求的高性能工作站, 及其他计算机接入交换机的 10Mb/s 专用端口, 以满足这类节点对专有传输速率的需求。

答案: 网络拓扑结构图如图 1.21 所示, 所有的传输媒体采用 5 类双绞线。

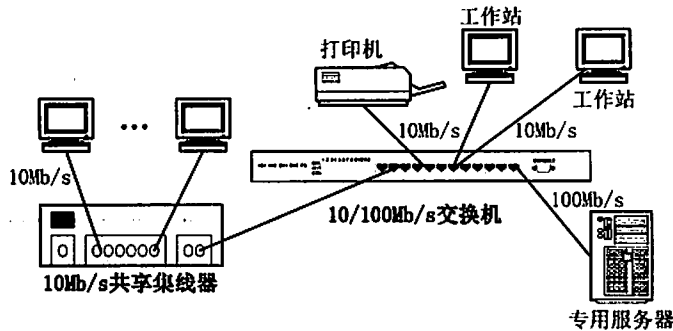


图 1.21 某实验室局域网拓扑结构图

例 10 阅读以下说明, 回答问题。

【说明】某中学校园网组网方案设计如下:

(1) 校园网组网环境:

一幢教学楼: 20 个教室, 每个教室连一台计算机; 2 个实验室, 每个实验室联 20 台计算机; 一幢办公楼: 10 个办公室, 每个办公室联 5 台计算机。两幢楼之间相距 105m。每幢楼内有一个设备间, 所有房间到设备间的距离均小于 90m。

(2) 根据需求, 拟采用 100BaseT 组网技术, 请选择适当的网络设备、传输介质, 并完成设计。

【问题 1】画出整个校园网的网络拓扑结构图, 并注明网络设备和传输媒体的名称、规格(速率、端口数)。

【问题 2】为实现办公信息发布、文件共享、师生交流、网上讨论和多媒体教学, 应配置什么服务器。

【问题 3】校园网接入 Internet 还要添加什么设备?

分析: 该校园网可采用 1 端口 100BaseFX 模块、24 个 10/100 BaseTX 自适应快速以太网端口交换机两个, 分别用于两楼之间互联, 两楼之间采用多模光纤相连。教学楼、办公楼各采用 1 台 48 口 10/100 BaseTX 自适应快速以太网端口交换机, 同时分别与带有光纤口的交换机进行级联。所有客户端机器分别采用超 5 类双绞线连接交换机端口。

为实现办公信息发布、文件共享、师生交流、网上讨论和多媒体教学, 应配置相应的部门级服务器(用户数 120 台左右), 可根据需求配置多个服务器。

同时为了实现校园网与 Internet 的互联, 应配备相应的路由器及防火墙设备。

答案:

【问题 1】网络拓扑结构图如图 1.22 所示。

【问题 2】为实现办公信息发布、文件共享、师生交流、网上讨论和多媒体教学, 应配置 Web 服务器、FTP 服务器、E-mail 服务器、BBS 服务器或 News 服务器、多媒体课件



视频流服务器(或多媒体服务器), 以上服务器均采用部门级服务器以上。也可根据需求将多个服务器合并成一个服务器。

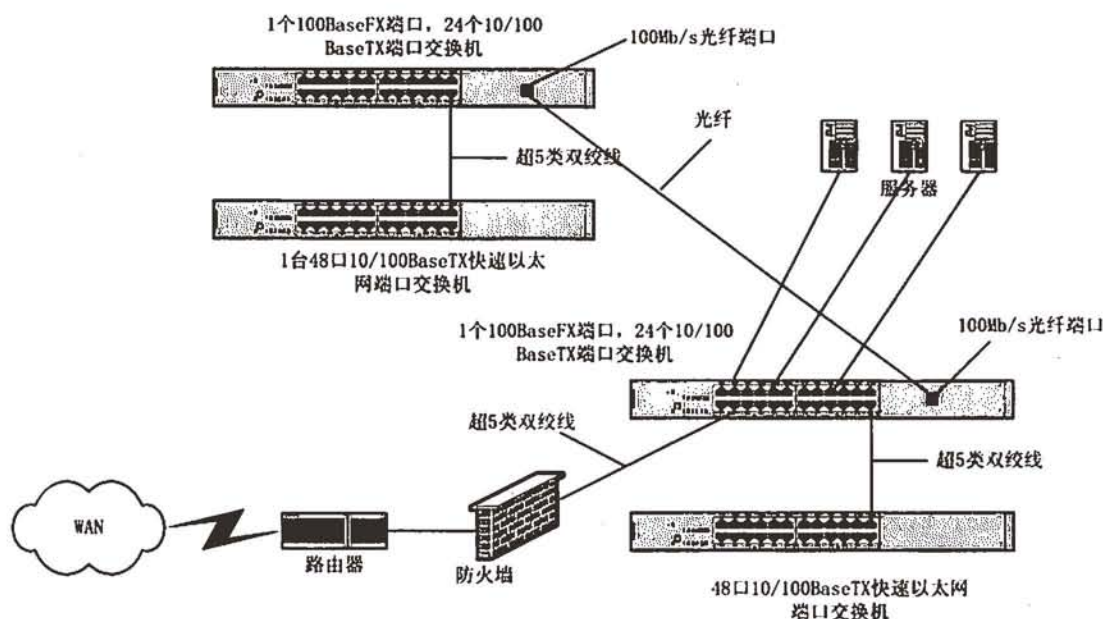


图 1.22 某中学局域网拓扑结构图

【问题 3】校园网接入 Internet 还要添加路由器和防火墙。

例 11 一宿舍有 8 台 PC 机, 但只有一个 Internet 端口, 可以同时满足每台 PC 机的上网要求。

分析: 由于网络规模较小, 考虑到经济原因, 用一个 8 口的 Hub 即可实现, (用其他方式实现也可)。将 8 台中的一台选作服务器配置两块网卡, 一块与 Hub 端口相连, 一块与 Internet 端口相连, 安装 Wingate 代理软件, 如安装 Win98 以上的操作系统, 则可直接配置 Internet 共享上网, 通过此连接, 可实现 8 台 PC 同时上网。

答案: 可采用一个 8 口的 Hub, 选择一台计算机配置两块网卡, 安装代理软件, 如 Wingate 等, 如操作系统为 Win98、Win2000、WinXP, 则可直接配置双网卡(如 Internet 共享上网)无须运行其他软件, 通过此连接, 可实现 8 台 PC 同时上网, 拓扑结构图如图 1.23 所示。

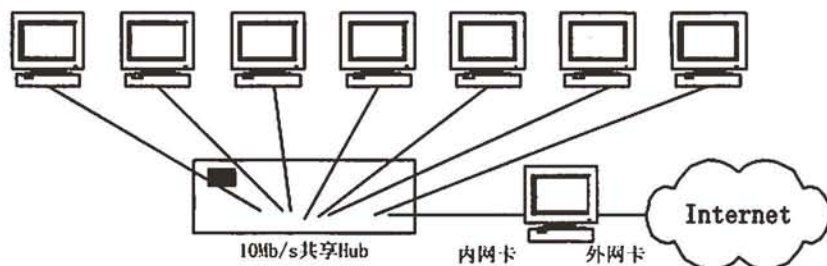


图 1.23 某宿舍局域网拓扑结构图

**例 12** 阅读以下的说明, 回答问题。

【说明】某单位原有一个 10Base5 和一个 10Base2 系统, 现需要再建一个 10BaseT 系统, 并要求将新建起来的 10BaseT 系统与原有的 10Base5 和 10Base2 系统相连。

【问题 1】10BaseT 以太网系统由哪几部分组成。它们之间通过什么连接器连接。

【问题 2】请指出连接所需设备和连接方法(含拓扑结构图)。

【问题 3】10Base5、10Base2、10BaseT 单段媒体的最长距离值。

【问题 4】最远两节点之间的距离值。

分析: 从传输介质看, 10Base 5、10Base 2 传输介质为同轴电缆, 10BaseT 为 UTP。从拓扑结构看, 10Base5、10Base2 为公共总线型结构, 10BaseT 为星型结构。

10Base5 粗缆以太网单根缆段的最大长度为 500m, 10Base2 细缆以太网单根缆段的最大长度为 185m, 10BaseT 连接方式使用不超过 100m 的双绞线将每一台网络设备连接到集线器上。

10BaseT 采用的中心设备是集线器 Hub, 如将 10Base5、10Base2 网络与 10BaseT 相连, Hub 上必须配置 AUI 及 BNC 连接器。

10BaseT 以太网系统由集线器、网卡以及双绞线组成。网卡与集线器之间通过 RJ-45 连接器连接双绞线, 一个 RJ-45 连接器最多可连接四对双绞线。

答案:

【问题 1】10BaseT 以太网系统由集线器、网卡和双绞线组成, 相互之间通过 RJ-45 连接器连接。

【问题 2】

(1) 连接设备: 10BaseT 集线器、双绞线、粗同轴电缆、细同轴电缆、BNC 和 AUI 接口、T 型头和收发器。

(2) 为满足工程要求, 10BaseT 采用的集线器产品必须配置 AUI 及 BNC 连接器, 当要与 10Base5 以太网连接时, 在集线器的 AUI 接口上配置一台外置收发器连接粗同轴电缆即可; 当要与 10Base2 以太网连接时, 在 10BaseT 集线器的 BNC 接口上配置 T 型头连接 10Base2 的基带细同轴电缆即可。其拓扑结构图如图 1.24 所示。

【问题 3】10Base5、10Base2、10BaseT 单段媒体的最长距离值分别是 500m、185m、100m。

【问题 4】最远两节点之间的距离值为 685(185+500)m。

**例 13** 阅读以下的说明, 回答问题。

【说明】某公司目前的网络拓扑结构如图 1.25 所示, 采用了具有中央集线器的以太网(各交换机之间采用 5 类双绞线相连), 由于网络节点的不断扩充, 各种网络应用日益增加, 网络性能不断下降, 因此该网络急需升级和扩充。

【问题 1】图 1.25 中集线器(Hub)最多可以串联几个?

【问题 2】为什么该网络的性能随着网络节点的扩充而下降? 分析一下技术原因?

【问题 3】共享型以太网系统存在的问题有哪几个?

【问题 4】如果要将该网络升级为 100Mb/s 交换型以太网, 应该如何解决?

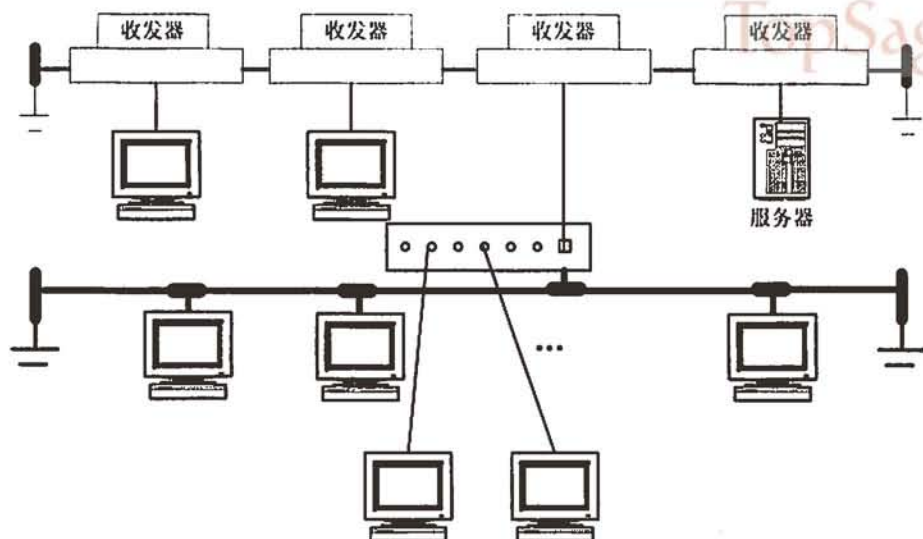


图 1.24 10Base5、10Base2、10BaseT 级联拓扑结构图

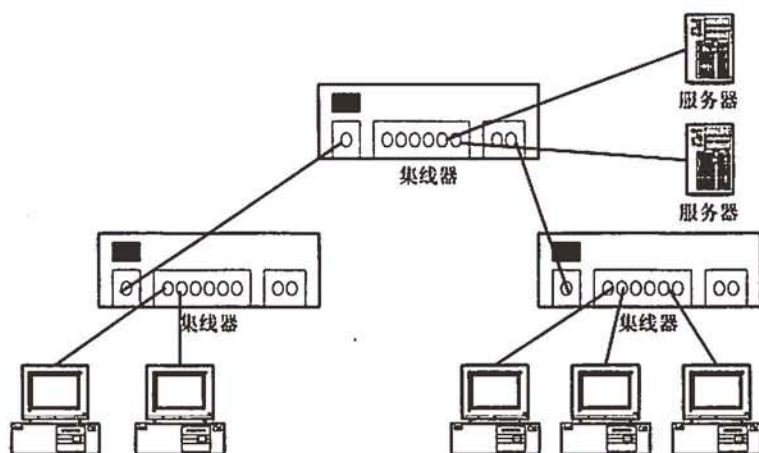


图 1.25 某公司网络拓扑结构图

【问题 5】如果在该网络中，所有客户机与服务器之间的通信非常频繁，为了克服入/出服务器通信量的瓶颈问题，该如何处理？

分析：对于规模较大，或节点(工作站)数超过单集线器的端口数目时，常采用多集线器的连接，这就是集线器的“级联”。级联的目的是为了组成更大规模的网络，级联结构的 10BaseT 网络遵循 5-4-3 规则，即任一条通路上的两台计算机间最多不能超过 5 段线，即最多可以串联 4 个集线器。3 个集线器能连接设备，2 个只能用于级联。网络上连接设备的总数不得超过 1024 台。

采用集线器结构的网络最大缺点在于它是一种共享介质的网络，随着网络节点的增加，冲突也会增加，网络的性能会随之急剧下降。

在提升网络性能时，最常用的方法是使用全双工交换机替代集线器，使网络性能大大提高。这是因为交换型以太网摒弃了传统以太网的 CSMA/CD 技术，而启用了先进的交换技术，从根本上消除了由于多个站点共享和竞争信道使用权而引发的碰撞现象。

答案:

【问题 1】集线器最多可以串联 4 个。

【问题 2】该网络采用了“共享式集线器”，即共享型网络，其工作原理是建立在“共享介质”基础上的，相应的介质访问控制方法是 CSMA/CD，这种控制方法保证了各节点能够公平地使用介质，即平分可用带宽。例如：某共享式以太网上的数据传输速率是 100Mb/s，当 10 个节点同时使用时，每个节点可以使用的最大传输速率就只有 10Mb/s。如果用户数量和通信超过一定数量时，将会造成碰撞，使得冲突增加。因此，共享型网络，在联网计算机的数目较少的时候，有较好的响应和性能；而在负荷较大时，将导致网络中计算机得到的带宽急剧减少，网络的传输速率和质量将迅速下降。

【问题 3】共享型以太网系统存在的问题有：

- (1) 受到 CSMA/CD 约束，一个碰撞域的带宽是固定的。
- (2) 站点越多时，每一站点的平均带宽越小。
- (3) 系统的带宽被多个群组所分割。
- (4) 由于数据的广播方式，数据安全性低。
- (5) 整个覆盖范围受到碰撞域的限制。

【问题 4】将上述集线器用带有部分 100Mb/s 端口的 10/100Mb/s 的交换机替代，所有级联口采用 100Mb/s 端口。

【问题 5】将服务器接入交换机的 100Mb/s 专用端口，以便得到专用的带宽和速率；如网卡为 10Mb/s，则将其更换为 100Mb/s，从而达到消除网络瓶颈的目的。

例 14 某网吧局域网，机器数量共为 16 台，现采用 ADSL 方式接入 Internet，应如何连接？请画出连接示意图，并列出硬件连接设备。

分析：局域网用户可通过 ADSL 接入 Internet，可选择网吧中的一台机器(插上两块网卡)做代理服务器，其中一块通过双绞线接 ADSL Modem 的 RJ-45 端口，设置相应的网络接入商提供的 IP 地址、子网掩码、DNS、网关等参数，另一块与交换机或集线器相连。服务器安装代理软件也可设置 Internet 共享上网(Windows 98 以上操作系统)，从而保证其他客户机通过代理上网。

答案：选择一台机器作为代理服务器，安装两块网卡，其中一块通过双绞线接 ADSL Modem 的 RJ-45 端口，设置网络接入商提供的 IP 地址、子网掩码、DNS、网关等参数，一块通过双绞线与交换机或集线器相连，并设置相应的私有地址，安装代理软件如 Wingate 或 Sygate 等(或用其他方式设置相应的代理)。如操作系统为 Win98、Win2000、WinXP，则可直接配置双网卡(如 Internet 共享上网)无须运行其他软件，通过此连接，保证局域网内其他客户机上网。其连接示意图如图 1.26 所示。

硬件连接设备有语音/数据分离器、ADSL 线路、ADSL 两芯电话线、ADSL Modem、代理服务器(两块网卡)、交换机或集线器、RJ-45 专线等。

例15 阅读以下说明，回答问题。

【说明】某公司内部有一个采用 TCP/IP 作为传输协议的 100BaseTX 局域网，包括 1 台服务器和 20 台客户机，通过一台 16 端口的交换机与一台 8 端口共享集线器级联，其网



络拓扑结构如图 1.27 所示。服务器上运行 DHCP 服务软件，客户机的 IP 地址由 DHCP 服务程序自动分配。

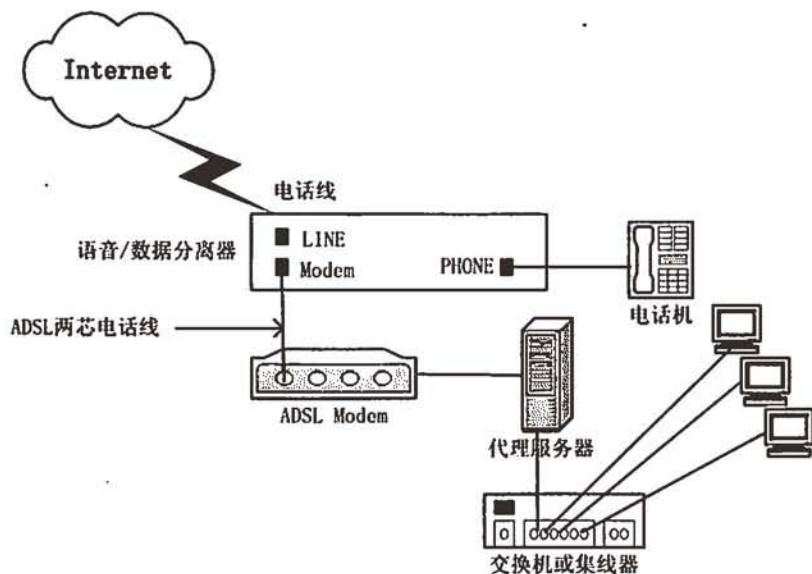


图 1.26 某网吧网络拓扑结构图

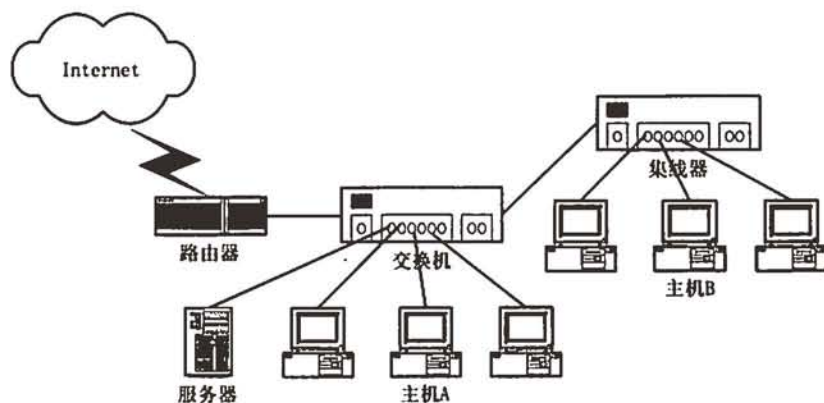


图 1.27 网络拓扑结构图

【问题 1】连接主机 A 与交换机的单根网线的最大长度为多少？

【问题 2】该局域网中的集线器每个端口平均享有的带宽是多少？

【问题 3】为了控制局域网用户访问 Internet 时只能进行 WWW 浏览，网管应该在路由器上采取什么措施？

【问题 4】100BaseTX 局域网中交换机最多可以级联几级？两个交换机间的距离不能超过多少米？

分析：双绞线的最大传输距离为 100m，如果电缆超长导致信号衰减过大，从而导致信号接收端无法正确识别信号，网络纠错功能要求发送端重新发送数据，如此反复，导致网络访问性能下降。故无论客户机通过双绞线连接集线器或交换机，还是交换机或集线器之间的级联都不能超过 100m。

集线器组建的以太网为共享型以太网系统。在整个系统中,受到 CSMA/CD 媒体访问控制方式的制约。整个系统处在一个碰撞域范围内,系统中每个站点都可能往媒体上发送帧,那么每个站点占用媒体的几率就是  $100\text{Mb/s}/n$ ,  $n$  为站数。

10BaseT 最多可以使用 4 个中继器或集线器连接 5 个 100m 长的网络段,如图 1.28 所示。而 100BaseTX 只允许使用 2 个,而且 2 个中继器或集线器之间的最大连接长度不能超过 5m。如图 1.29 所示。

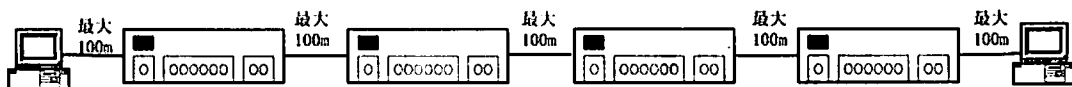


图 1.28 10BaseT 级联示意图

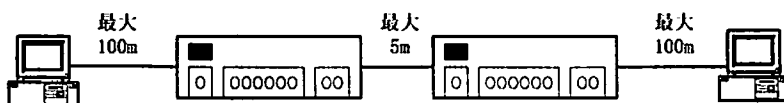


图 1.29 100BaseT 级联示意图

路由器具有防火墙功能。路由器通常有多种隔离信息包的方法,从而进一步加强网络的安全保密性,防止网络系统和系统内数据遭到攻击和破坏。

答案:

【问题 1】100m

【问题 2】 $100\text{Mb/s} \div 8 = 12.5\text{Mb/s}$

【问题 3】在路由器上做策略限制,仅让 TCP 的 80 端口能够进行数据包传输。

【问题 4】2 级; 100m

### 1.2.3 同步练习

1. 简要回答下列有关局域网的问题。

【问题 1】局域网需要 OSI 参考模型的哪几层?

【问题 2】局域网的标准主要是由哪个委员会制定的?

【问题 3】列出局域网常用的访问控制方式?

2. 简要回答下列有关 10Mb/s 以太网的问题。

【问题 1】简述 10BaseT 以太网的组成。

【问题 2】简述 10BaseT 以太网系统的特点。

【问题 3】在 10BaseT 的收发器中,双绞线起什么作用?

【问题 4】试比较四种 10Base 以太网的物理性能。

3. 按传输媒体类型划分快速以太网类型。

4. 交换型以太网的中心设备是什么?与共享型以太网系统比较,交换型以太网系统有何特点?

5. 10 Mb/s 以太网、快速以太网以及千兆位以太网有何区别与联系。

6. 对于工作在半双工模式的 24 口交换机,若每个端口的速率为 10Mb/s,则整个系统带宽可达多少?

7. 简要回答下列问题。

【问题 1】哪些以太网产品支持全双工操作？

【问题 2】简述全双工以太网的技术特点(与传统半双工以太网相比)。

8. 已知某局域网采用 CSMA/CD 媒体访问控制技术, 其共享媒体最大跨距为 500m, 物理层处理延迟时间为  $10^{-5}$ s, 传输媒体的数据传输率为 10Mb/s, 试计算该网络的最小帧长度。

9. 简要回答下列问题。

【问题 1】收发器的主要功能有哪些？

【问题 2】对于 10Mb/s 的以太网有哪几种收发器？

【问题 3】集线器在以太网系统中具有的主要功能。

10. 简要回答下列问题。

【问题 1】1000BaseT 有何特点？

【问题 2】100BaseTX/FX 系统的跨距技术要点。

【问题 3】千兆位以太网跨距的技术要点。

11. 根据设备在如图 1.30 所示的网络系统中的作用, 正确标出图中被编号设备的名称。

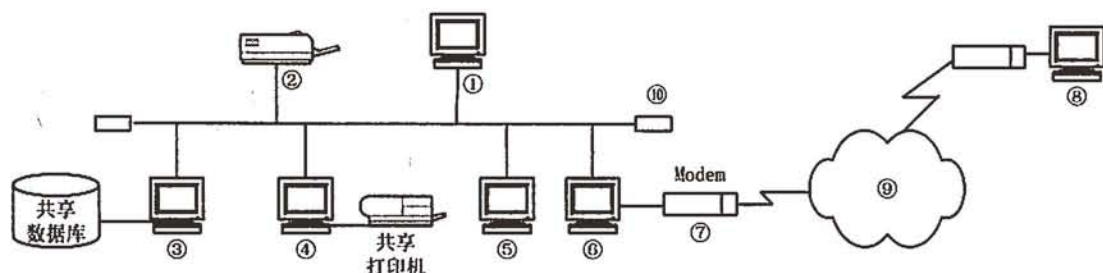


图 1.30 网络系统拓扑结构图

## 1.2.4 同步练习参考答案

1.

【问题 1】局域网需要 OSI 中的物理层、数据链路层(数据链路层分为媒体访问控制子层和逻辑链路控制子层)。

【问题 2】IEEE 802 委员会

【问题 3】局域网常用的访问控制方式有 3 种, 分别是载波帧听访问/冲突检测(CSMA/CD)、令牌环访问控制法(Token Ring)和令牌总线访问控制法(Token Bus)。

2.

【问题 1】10BaseT 以太网的组成:

(1) 10BaseT 以太网系统由集线器、网卡、非屏蔽双绞线(3 类以上)组成。

(2) 网卡与集线器、集线器之间通过 RJ-45 连接器和双绞线实现互联和通信。

(3) 10BaseT 以太网系统中, 单段媒体最大长度为 100m, 可以通过 4 个集线器级联, 连接 5 个媒体使最大跨距达 500m。

【问题 2】10BaseT 以太网系统的特点:

- (1) 采用星型或树型拓扑结构, 核心为集线器。
- (2) 传输媒体采用 3、4 或 5 类非屏蔽双绞线, 发送与接收通道物理上分开, 各占一根双绞线。

(3) 网络站点通过网卡上的 RJ-45 连接器和双绞线直接连接集线器。

**【问题 3】双绞线作用:**

(1) 网卡上发送和接收分别使用一根双绞线, 即一根双绞线发送信号, 另一根作为信号接收使用。

(2) 当网卡与集线器相连接时, 网卡上作为发送的那根双绞线正作为集线器接收使用; 反之, 网卡上作为接收的那根双绞线正作为集线器发送使用。

**【问题 4】10Base 以太网的物理性能:**

(1) 10Base5 使用外置收发器, 传输媒体为价格较贵、需要专业化安装的直径 10mm、阻抗 50 $\Omega$  的粗同轴电缆, 采用总线型拓扑结构, 单段媒体最大长度为 500m, 最多可使用 4 个中继器连接 5 段媒体使跨距最大达 2.5km, 网卡通过 AUI 接口与媒体连接。

(2) 10Base2 在网卡上内置收发器, 传输媒体使用价格便宜、安装简单的直径 5mm、阻抗 50 $\Omega$  的细同轴电缆, 采用总线型拓扑结构, 单段媒体最大长度为 185m, 最多可使用 4 个中继器连接 5 段媒体使跨距最大达 925m, 网卡通过 BNC 连接器和 T 型头与媒体连接。

(3) 10BaseT 在网卡上内置收发器, 传输媒体使用便宜、安装简单的非屏蔽双绞线(3 类以上 UTP), 采用星型拓扑结构, 单段媒体最大长度为 100m, 可以通过 4 个集线器级联, 连接 5 个媒体使最大跨距达 500m, 网卡通过 RJ-45 连接器与媒体连接。

(4) 10BaseF 在网卡上内置收发器, 传输媒体使用 62.5/125 多模光纤, 采用星型拓扑结构, 单段媒体最大长度为 2km, 可以通过 1 个集线器级联, 连接 2 个媒体段使最大跨距达 4Km, 网卡通过 ST 连接器与光纤连接。

**3.**

(1) 按传输媒体类型划分, 快速以太网可分为 100BaseTX、100BaseFX、100BaseT4 3 种类型。

(2) 100BaseTX 采用 5 类非屏蔽双绞线, 使用 2 对线对。

(3) 100BaseFX 采用多模光纤或单模光纤。

(4) 100BaseT4 采用 3 类非屏蔽双绞线, 使用全部 4 对线对。

4. 交换型以太网的中心设备是以太网交换机。交换型以太网系统与共享型以太网比较有如下优点:

(1) 每个端口上可以连接站点, 也可以连接一个网段。不论站点和网段均独占该端口的带宽。

(2) 系统的最大带宽可以达到端口带宽的  $n$  倍, 其中  $n$  为端口数。 $n$  越大, 系统的带宽越高。

(3) 交换机连接了多个网段, 每一个网段都是独立的, 被隔离的。但如果需要的话, 独立网段之间通过其端口也可以建立暂时的数据通道。

(4) 被交换机隔离的独立网段上数据流信息不会随意广播到其他端口上去, 因此具有一定的数据安全性。

**5.**



(1) 快速以太网和千兆位以太网属于高速以太网,是在 10Mb/s 以太网基础上发展起来的、数据传输率更高的以太网技术。

(2) 快速以太网是在 10BaseT 和 10BaseF 技术基础上发展起来的具有 100Mb/s 数据传输率的以太网,快速以太网的传输媒体和媒体布局向下兼容 10Mb/s 以太网,帧结构和媒体访问控制方式则完全按照 IEEE 802.3 基本标准。

(3) 千兆位以太网是快速以太网的自然发展,只是数据传输率达到 1000Mb/s,二者的拓扑结构完全一致,传输媒体的媒体布局在快速以太网基础上有所发展,但向下兼容快速以太网和 10Mb/s 以太网,帧结构和媒体访问控制方式也与 IEEE 802.3 基本类同,但有所发展。

6. 240Mb/s(24×10Mb/s)

7.

【问题 1】(1)只有链路上提供独立的发送和接收媒体的以太网产品才能支持全双工操作。

(2) 在 10Mb/s 以太网中只有 10BaseT 和 10BaseF 支持全双工操作。

(3) 在 100Mb/s 以太网中 100BaseTX、100BaseFX 都支持全双工操作。

(4) 在 1000Mb/s 以太网中 1000BaseLX、1000BaseSX、1000BaseCX、1000BaseTX 都支持全双工操作。

【问题 2】全双工以太网技术是用来说明以太网设备端口的传输技术,与传统半双工以太网技术区别在于:每个端口和交换机背板之间都存在两条逻辑通路。这样,每一个端口就可以同时接收和发送帧,不再受到 CSMA/CD 的约束,在端口发送帧时不再会发生帧的碰撞,已无碰撞域的存在。这样一来,端口之间媒体的长度仅仅受到数字信号在媒体上传输衰变的影响,而不像传统以太网半双工传输时还要受到碰撞域的约束。

8. 根据最小帧长度的计算公式:

$$\begin{aligned} L_{\min} &= \text{slot time} \times R \approx (2S/0.7C + 2t_{\text{inv}}) \times R \\ &= (2 \times 500 / (0.7 \times 3 \times 10^8) + 2 \times 10^{-5}) \times 10 \times 10^6 \\ &= 248(\text{位}) \end{aligned}$$

所以该网络最小帧长度为 248 位。

9.

【问题 1】收发器的主要功能有:向媒体发送信号、自媒体接收信号、识别媒体是否存在信号。

【问题 2】对于 10Mb/s 的以太网有 10Base5、10Base2、10BaseT、10BaseF 几种收发器。

【问题 3】集线器在以太网系统中具有的主要功能有:一是媒体上信号的再生和再定时,二是检测碰撞,三是端口的扩展功能,四是混合连接 10Base5 与 10Base2 以太网系统。

10.

【问题 1】1000BaseT 的特点是:使用 5 类 UTP、标准为 IEEE 802.3ab、最长的媒体距离达 100m、采用专门的更先进的编码/译码方案和特殊的驱动电路方案,可以在原来使用 5 类 UTP 的布线系统中,传输的带宽可升级 10 倍。

【问题 2】100BaseTX/FX 系统的跨距:在双绞线媒体情况下,由于最长媒体段跨距离

为 100m, 加 1 个中继器可延伸 1 个最长媒体段距离, 达到 200m; 如果再想延伸距离时, 加 1 个中继器后, 只能达到 205m, 205m 即为快速以太网的跨距。

在光缆媒体情况下, 不使用中继器, 跨距可达 412m, 即是 1 个碰撞域范围, 但光缆的最长媒体段要远远大于 412m。加了中继器后, 并不能延伸距离, 由于中继器的延迟时间, 因此反而跨距变小了。

【问题 3】千兆位以太网组网跨距的技术要点:

无中继器连接。

(1) 在采用光缆和铜缆两种媒体时差别很大。即仅采用了光缆作为媒体, 还要区分多模还是单模光纤, 多模光纤还有 50 $\mu$ m 和 62.5 $\mu$ m 之分, 驱动光源还有长短波之分。

(2) 采用铜缆要区分是屏蔽双绞线还是 5 类非屏蔽双绞线。

(3) 要区分是在半双工模式还是全双工模式下联网。

中断器连接。

(1) 采用铜缆媒体时, 使用 1 个中继器, 跨距能增加 1 倍。而在采用光缆媒体时跨距反而减少。

(2) 采用光缆时, 半双工的跨距已反映了碰撞域的最大范围。加 1 个中继器后, 在半双工模式下, 跨距分别为: 1000BaseLX/SX 为 240m; 1000BaseCX 为 50m; 1000BaseT 为 200m。

- |          |        |           |
|----------|--------|-----------|
| 11. ①客户机 | ②网络打印机 | ③数据库服务器   |
| ④打印服务器   | ⑤客户机   | ⑥客户机      |
| ⑦调制解调器   | ⑧远程客户机 | ⑨Internet |

## 1.3 以太网交换机的部署、配置和管理

### 1.3.1 考点辅导

#### 1.3.1.1 以太网交换机的部署

交换机的连接模式有级联模式、堆叠模式和混合模式。

##### 1. 级联模式

级联模式是最常规、最直接的一种扩展方式。级联模式是通过双绞线或光纤, 一般在交换机的前面板上有专门的级联口, 如果没有, 也可以用交叉线接法来级联。级联是通过端口进行的, 级联后两台交换机是上下级的关系。

级联模式起源于早期的共享型集线器(Hub), 共享型集线器的物理拓扑结构是星型的, 而逻辑拓扑结构是总线型的。集线器仅仅相当于一条浓缩的总线, 在集线器的某一个端口级联另一台集线器, 只是相当于把浓缩的总线又加长了一些, 但其仍然是一条总线, 所有端口都要在一个碰撞域里受到 CSMA/CD 的约束。但这样相当于把传输媒体加长了, 在加长的传输媒体上又增加了一些端口。但付出的代价是, 在这个碰撞域里, 又多了一些端口共享整个带宽, 从而导致网络性能低下。当然这种级联方式, 必须遵循 5-4-3 法则, 也就

是级联不能超过4层。

在交换机上进行级联，级联交换机的端口共享的仅仅是被级联交换机端口的带宽，而不是整个网络的带宽。更何况目前的交换机级联通常是高速交换机级联低速交换机，即1000Mb/s 端口级联 100/1000Mb/s 的交换机；100Mb/s 端口级联 10/100Mb/s 的交换机；或者是交换机级联共享型的集线器。由此一来，极大程度地克服了传统集线器级联共享带宽，而导致网络性能降低的弊端。

## 2. 堆叠模式

堆叠通常是为了扩充带宽用的，通常用专门的堆叠卡插在交换机的后面，用专门的堆叠电缆连接几台交换机，堆叠后这几台交换机相当于一台交换机。堆叠是采用交换机背板的叠加，使多个工作组交换机形成一个工作组堆，从而提供高密度的交换机端口的，堆叠中的交换机就像一个交换机一样，配制一个IP地址即可。

级联是通过交换机的某个端口与其他交换机相连的，而堆叠是通过集线器的背板连接起来的，它是一种建立在芯片级上的连接，如两个24口交换机堆叠起来的效果就像是一个48口的交换机。

常见的堆叠有两种：菊花链堆叠和矩阵堆叠。

## 3. 混合模式

在实际的应用中，由于网络的复杂性，用户需求的多重性，通常同时使用两种模式进行交换机的部署，称其为混合模式。

### 1.3.1.2 以太网交换机的设置

对一台新的交换机进行配置和管理有两个主要步骤，一是通过仿真终端进行IP地址设置，二是通过浏览器进行管理。

#### 1. 通过仿真终端进行IP地址设置

通过仿真软件设置3COM交换机IP地址的步骤如下：

- (1) 用一条RS-232型电缆将管理终端的串口与交换机的控制台端口(Console)相连。
- (2) 运行仿真终端软件，通常使用【附件】中的【超级终端】即可。
- (3) 选择所连接的串口，如COM1端口。
- (4) 根据说明书设置仿真终端的位率、数据位、奇偶校验和停止位等参数。
- (5) 设置远程登录的用户名、密码及其他常见用户名。
- (6) 设置IP地址及子网掩码。

#### 2. 通过浏览器进行管理

(1) 打开浏览器，在URL栏中输入交换机IP地址后按回车键，出现交换机的Web登录界面，在Web登录界面中输入相应的用户名和密码后，单击【确定】按钮。

(2) 进入交换机的Web管理页面。

(3) 在Web管理页面中，既可以查看交换机的基本信息，也可以进行一些参数设置，如修改交换机管理用户的口令。

### 1.3.2 典型例题分析

**例 1** 以太网交换机一定要设置才能工作, 是否正确?

**分析:** 一台新的交换机部署到网络中后, 使用默认配置就可以工作, 不需要再进行设置。因为它是一种将软件装在 FlashMemory(闪存)中的硬件设备, 当加电时, 首先进行一系列自检, 对所有的端口进行测试之后, 交换机就处于工作状态。这时设备的交换表是空的, 它可以通过自学来了解各个端口的设备连接情况, 并将设备的 MAC 地址记录在交换表中, 当有信息交换时, 交换机就根据交换表来进行数据转发。

但是, 当有一些高级应用和需求时, 例如, 通过交换机划分 VLAN, 或是对交换机进行远程管理等, 就需要对交换机进行设置。

**答案:** 错误, 以太网交换机在一般应用时, 不需进行任何设置即可使用。

**例 2** 交换机之间级联只能采用双绞线, 是否正确? 采用什么类型的级联双绞线?

**分析:** 交换机之间级联可通过双绞线或光纤。用双绞线进行级联时, 可根据实际情况采用直通线或交叉线。

**答案:** 错误。级联双绞线可根据需要采用直通线或交叉线。

**例 3** 非屏蔽双绞线的直通线和交叉线可用于下列哪两种设备间的通信, 集线器到集线器(不使用级联端口)使用 (1); PC 到集线器使用 (2); PC 到交换机使用 (3); PC 到 PC 使用 (4)。

**分析:** 对于那些没有专用级联端口的集线器之间的级联, 双绞线接头中线对的分布与连接网卡和集线器有所不同, 必须要用交叉线。而许多集线器为了方便用户, 提供了一个专门用来连接到另一台集线器的普通端口, 对此类集线器进行级联时, 双绞线均采用直通线。

**答案:** (1)交叉线 (2)直通线 (3)直通线 (4)交叉线

**例 4** 交换机与集线器(Hub)如何进行级联才能达到最佳效果。

**分析:** 在 Hub 和交换机性能优化方面主要体现在 Hub 或交换机的级联上。如果需要 Hub 与 Hub 或 Hub 与交换机级联, 则一定要注意 Hub 的带宽是所有端口共用的, 因此每个端口实际利用的带宽则是应用总带宽(如 100M)除以所用端口数。所以一般不用 Hub 来级联, 而是通过用 Hub 连接在交换机的端口上, 因为交换机所指的带宽就是每个端口的实际可用带宽, 如  $n10M+m100M$ , 就表明在这个交换机上有  $n$  个 10M 的带宽, 有  $m$  个 100M 的带宽端口, 这些带宽是具体端口独享的, 而不受交换机所用端口数的限制。

也就是说, 如果一个 Hub 连在一个交换机的 100M 端口上, 则这个 Hub 上就拥有总共 100M 的带宽; 如果一个 Hub 连接在有 100M 带宽的 Hub 端口上, 则连接一个 Hub 可能使用了 10 个端口, 实际上下一个 Hub 的总带宽就远达不到 100M 的带宽, 这样就影响了连接在下一个 Hub 上的工作站速度。所以 Hub 级联一般最多为两层, 层数多了会使速度呈倍差级数减慢。

另外还有两点要注意, 其一是, 当 Hub 要通过交换机级联时最好连接在 100M 带宽的



端口, 除非没有 100M 端口可用了; 其二是, 要注意双绞线最大单段网线长度在 100 米以内, 否则信号会衰减严重, 影响网络速度。

答案: 一个 Hub 连在一个交换机的 100M 或 10M 端口上, 同时相互级联的网线长度在 100m 之内。

例 5 连接以太网交换机的模式有两种: 级联和堆叠, 其中堆叠模式\_\_\_\_。(2004 年下半年网络管理员上午试卷 38)

- A. 仅有菊花链堆叠
- B. 既可以菊花链堆叠, 又可以矩阵堆叠
- C. 仅有矩阵堆叠
- D. 并联堆叠

分析: 堆叠的目的通常是扩充带宽, 通常用专门的堆叠卡插在交换机的后面, 用专门的堆叠电缆连接几台交换机, 堆叠后这几台交换机相当于一台交换机。堆叠是采用交换机背板的叠加, 使多个工作组交换机形成一个工作组堆, 从而提供高密度的交换机端口的, 堆叠中的交换机就像一个交换机一样, 配制一个 IP 地址即可。级联是通过交换机的某个端口与其他交换机相连的, 而堆叠是通过集线器的背板连接起来的, 它是一种建立在芯片级上的连接, 如 2 个 24 口交换机堆叠起来的效果就像是一个 48 口的交换机。常见的堆叠模式有两种: 菊花链堆叠和矩阵堆叠。

答案: B

### 1.3.3 同步练习

1. 什么是级联?
2. 简述级联的优势?
3. 常见的堆叠有哪两种? 堆叠技术的最大优点是什么?
4. 简述堆叠模式的优、缺点?
5. 在网络中利用以太网交换机进行部署时, 常采用哪三种模式?
6. 对没有任何设置的交换机通过何种方式进行配置?
7. 设置了 IP 地址以后的交换机可采用哪两种方式进行远程管理?
8. 描述通过仿真软件设置 3COM 交换机 IP 地址的步骤?
9. 通过 Web 页面可对设置 IP 地址的 3COM 3300 交换机进行远程管理, 请列举出通过远程管理可实现哪些功能?

### 1.3.4 同步练习参考答案

1. 级联是通过双绞线或光纤把需要级联的设备通过端口相连接, 从而达到增加同一网络端口数目的方法。

2. 级联的优势有:

(1) 级联模式可使用通用的以太网端口进行层次间互联, 其中包括 100Mb/s 端口、1000Mb/s 端口以及新兴的 10Gb/s 端口。

(2) 级联模式是组建结构化网络的必然选择,级联使用普通的、长度限制并不严格的电缆(光纤),各个级联单元的位置相对较随意,非常有利于综合布线。

(3) 级联模式通常是解决不同品牌的交换机之间以及交换机与集线器之间连接的有效手段。

3. 常见的堆叠有两种:菊花链堆叠和矩阵堆叠。堆叠技术的最大的优点就是提供简化的本地管理,将一组交换机作为一个对象来管理。

4. 堆叠模式的优点是:

(1) 增加网络端口的同时,还增加了逻辑通道,扩充了网络带宽,不同堆叠单元的端口之间可以直接交换,进行快速转发,从而极大地提高了网络性能。

(2) 不受 5-4-3 法则的约束,堆叠单元可以超过 4 个。

(3) 提供简化的本地管理,将一组交换机作为一个对象来管理。

堆叠模式的缺点是:

(1) 堆叠是一种非标准化技术,各个厂商之间不支持混合堆叠,同一组堆叠交换机必须是同一品牌。

(2) 堆叠模式不支持即插即用,在物理连接完毕之后,还要对交换机进行相应的设置,才能正常运行。

(3) 不存在拓扑管理,一般不能进行分布式布置。

5. 采用三种模式:级联模式、堆叠模式、混合模式。

6. 对没有任何设置的交换机通过仿真终端可设置交换机的登录用户名、密码、IP 地址及子网掩码等。

7. 交换机可通过 Telnet 命令行的方式及 Web 页面的方式进行远程管理。

8. 设置步骤如下:

(1) 用一条 RS-232 型电缆将管理终端的串口与交换机的控制台端口(Console)相连。

(2) 运行仿真终端软件如(超级终端)。

(3) 选择所连接的串口。

(4) 根据说明书设置仿真终端的位率、数据位、奇偶校验和停止位等参数。

(5) 设置远程登录的用户名、密码及其他常见用户名。

(6) 设置 IP 地址及子网掩码。

9. 远程管理可实现如下功能:

(1) 可查看联入交换机机器网卡的 MAC 地址。

(2) 可查看每一个端口的状态。

(3) 可根据需要关闭、打开端口。

(4) 可以修改交换机管理用户的口令。

(5) 可根据需要对端口进行 VLAN 的划分等。

## 1.4 VLAN 的划分

### 1.4.1 考点辅导

#### 1.4.1.1 以太网中划分 VLAN

##### 1. VLAN 的概念

VLAN(Virtual Local Area Network)的中文名称为“虚拟局域网”，VLAN是为了解决以太网广播问题 and 安全性而提出的一种协议，它在以太网帧的基础上增加了 VLAN 头，用 VLAN ID 把用户划分为更小的工作组，限制不同工作组间的用户互访，每个工作组就是一个虚拟局域网。虚拟局域网的好处是可以限制广播范围，并能够形成虚拟工作组，动态地管理网络。

##### 2. VLAN 的分类

###### (1) 基于端口划分的 VLAN

将交换设备端口进行分组以划分 VLAN。

按交换端口划分 VLAN 是构造 VLAN 最常用的方法。其特点是：划分方法简单有效，VLAN 可以跨越多个交换设备；但同一个交换端口无法同时参与多个 VLAN；当客户从一个端口迁移到另一个端口后需要重新配置 VLAN。

###### (2) 基于 MAC 地址划分的 VLAN

由网管人员指定属于同一个 VLAN 的各客户站的 MAC 地址，按照 MAC 地址划分 VLAN。

按 MAC 地址划分的 VLAN 可以看作是基于用户的 VLAN。其特点是：客户的迁移不需要重新配置 VLAN，同一个 MAC 地址可以同时属于多个 VLAN；但 VLAN 初始的手工配置不太容易；共享媒体环境下实现的基于 MAC 地址的 VLAN，在多个不同 VLAN 的成员同时存在于同一个交换端口时会导致性能下降严重；在大规模的基于 MAC 地址的 VLAN 中，交换设备之间进行 VLAN 成员身份信息的交换也会引起性能降低。

###### (3) 基于网络层协议划分的 VLAN

根据协议类型或网络层地址来划分 VLAN。

其优点是：用户的物理位置改变了，不需要重新配置所属的 VLAN，而且可以根据协议类型来划分 VLAN。另外，这种方法不需要附加的帧标签来识别 VLAN，这样可以减少网络的通信量。

其缺点是：对报文中的网络地址进行检查的开销比较大，将引起 VLAN 性能下降。

按网络层协议划分的 VLAN 反对 TCP/IP 协议特别有效。

###### (4) 根据 IP 组播划分的 VLAN

IP 组播实际上也是一种 VLAN 的定义，即认为一个组播就是一个 VLAN，这种划分的方法将 VLAN 扩大到了广域网，因此这种方法具有更大的灵活性，而且也很容易通过路由器进行扩展，当然这种方法不适合局域网，主要因为它的效率不高。

### 3. VLAN 的功能

VLAN 的功能包括：提高管理效率、控制广播数据、增加网络安全性、减少站点的移动和改变开销、实现虚拟工作组。

#### (1) 提高管理效率

VLAN 为控制网络中站点的移动、增加和改变而进行修改时的工作提供了有效的手段，同时对交换机和路由器重新进行配置的开销将得以减少。例如当某个 VLAN 中的一个用户从一个地点移动至另一个地点时，只要他们仍旧保持在同一个 VLAN 中并且能够连接到一个交换机的端口上，就无须对他们的网络地址进行修改，最多只是需要将此端口重新配置到相应的 VLAN 中。此种方式将极大的简化配置和调试工作，并且此时路由器的配置可以保持不变。

在 VLAN 解决方案中一般都带有可集中配置管理和监控的 VLAN 管理软件，可以进行站点的移动、增加和修改以及网络资源访问权限的设置等。

#### (2) 控制广播数据

在同一个 VLAN 中的工作站，不论它们实际与哪一个交换机连接，它们之间的通信就好像在独立的交换机上一样。同一个 VLAN 中的广播只有 VLAN 中的成员才能听到，而不会传输到其他的 VLAN 中去，这样可以很好地控制广播风暴的产生。

#### (3) 增加网络安全性

增强网络安全性的一种最有效和最易于管理的方法是将整个网络划分成一个互相独立的广播组(VLAN)。另外网管人员可限制某个 VLAN 中的用户的数量，并且可以禁止那些没有得到许可的用户加入到某个 VLAN 中。按照此种方式，VLAN 可以提供一道安全性防火墙，以控制用户对于网络资源的访问，控制广播组的大小和构成，并且可借助于网管软件在发生非法入侵时及时通知管理人员。

#### (4) 减少站点的移动和改变开销

VLAN 可以减少处理用户站点的移动和改变所带来的开销。因为 VLAN 的成员身份同站点所在的地址是无关的，这样一来站点可以发生移动而其 IP 地址和子网成员身份则可以保持不变。

#### (5) 实现虚拟工作组

虚拟工作组指的是当在整个园区网络环境中实现了 VLAN 之后，同一个部门的所有成员将可以像处于同一个 LAN 上那样进行通信，大部分网络通信将不会传出此 VLAN 广播域。当某个用户从一个地方移动到另一个地方时，如果用户的工作部门发生变化，用户可以不改变其工作地点，而只需网管人员修改一下其 VLAN 成员身份即可。

### 4. VLAN 配置实例

主要了解 3COM 的 Switch 3300 交换机的配置情况。

#### 1.4.1.2 三层交换

##### 1. 三层交换技术

三层交换，又称多层交换或 IP 交换，是将传统交换器与传统路由器结合起来的网络设备，它即可以完成传统交换机的端口交换功能，又可以完成部分路由器的路由功能。简单



地说,三层交换技术就是:“二层交换技术+三层转发技术”。

## 2. 三层交换技术的实现

几种广泛应用的三层交换技术:

- (1) 3COM 的 Fast IP。
- (2) 3COM 的 FIRE。
- (3) Cisco 的 NetFlow。
- (4) Cisco 的标记交换。

## 3. 三层交换技术的应用

在局域网内可以利用三层交换机代替传统的路由器以提高性能。

# 1.4.2 典型例题分析

例1 阅读以下说明,回答问题。

【说明】某一公司组建了三层交换局域网,公司网管部按业务部门划分了多个 VLAN,即一个部门形成一个虚拟局域网,该公司所属人员办公地点经常因工作需要变动。

【问题1】三层交换设备是一个什么样的设备。

【问题2】简述虚拟局域网的功能。

【问题3】说明按交换端口划分 VLAN 和按 MAC 地址划分 VLAN 的各自特点。

【问题4】该公司如何划分 VLAN。

分析:本题考查的是一是三层交换技术,三层交换技术是“二层交换技术+三层转发技术”;二是考查虚拟局域网的功能,即控制广播数据、提高管理效率、增加网络安全性、减少站点的移动和改变开销、实现虚拟工作组;三是考查基于端口划分的 VLAN、基于 MAC 地址划分的 VLAN 的特点。

答案:

【问题1】三层交换设备是一个带有路由功能的设备,因此用三层交换技术来实现 VLAN 互联是一个很好的选择。

【问题2】虚拟局域网的功能有控制广播数据、提高管理效率、增加网络安全性、减少站点的移动和改变开销、实现虚拟工作组。

【问题3】按交换端口号划分:交换机1和交换机2上端口1,2,3,6与1,7,8所连接的客户站构成 VLANA。而相应的端口4,5,6,7与4,5,6所连接的客户构成 VLANB。但仅靠端口分组而定义 VLAN 将无法使得一个物理分段同时参与到多个 VLAN 中,而且更要紧的是当一个客户站从一个端口移至另一个端口时,网管人员将不得不对 VLAN 成员进行重新配置。

按 MAC 地址划分:是由网管人员指定属于同一个 VLAN 中的各客户站的 MAC 地址,移至网络中另外一个地方时 MAC 地址仍保持其原先的 VLAN 成员身份而无须网管人员对其进行重新配置。不足在于所有的用户在最初都必须被配置到至少一个 VLAN 中,只有在此种手工配置之后方可实现对 VLAN 成员的自动跟踪。

【问题4】由于该公司人员工作人员办公地点经常迁移,故应按 MAC 地址划分 VLAN。

**例 2** 请回答下列有关 VLAN 的问题。

**【问题 1】** VLAN 基本上可以看成是一个什么域？

**【问题 2】** 为了增强网络的安全性，网管人员可以禁止什么样的用户加入到某个 VLAN 中。

**【问题 3】** 有了虚拟工作组功能后，如果某个用户改变了工作部门，它可以不改变其工作站点，网管人员如何做。

**分析：**一个 VLAN 可以看成是一组客户工作站的集合。这些工作站不必处于同一个物理网络上，它们可以不受地址位置的限制像处于同一个 LAN 上那样进行通信和信息交换。VLAN 基本上可以看成是一个广播域。

一个 VLAN 可以看成是一组客户工作站的集合。这样工作站不必处于同一个物理网络上，它们可以不受地理位置的限制，就像处于同一个 LAN 上那样进行通信和信息交换。为了增加网络的安全性，只有得到网络人员许可的用户才能加入到某个 VLAN 中。

每一个 VLAN 都包括了相应的客户站。可以认为一个 VLAN 实际上是逻辑上的网段。如果某个用户改变了工作部门，他可以不改变其工作站点，只需网管人员为其修改 VLAN 成员身份即可。这种逻辑上的网段给 LAN 管理、安全性以及广播数据的抑制带来诸多的益处。

**答案：**

**【问题 1】** 广播域

**【问题 2】** 没有得到许可

**【问题 3】** 修改 VLAN 成员身份

**例 3** 请给出下面利用 VLAN 的解决方法。

**【问题 1】** 工程部有机密文件需要保密。

**【问题 2】** 销售部门的笔记本用户经常需要从外地进行拨号访问 VLAN。

**【问题 3】** 公司安装了视频培训服务器，要防止用户做视频访问时占用太多的带宽。

**【问题 4】** 公司总裁需要能访问财务、销售等其他部门的 VLAN。

**分析：**VLAN 的分类有基于端口划分的 VLAN、基于 MAC 地址划分的 VLAN、基于网络层协议划分的 VLAN、根据 IP 组播划分的 VLAN。根据以上 VLAN 的划分，可根据需求选择一种方法对用户端划分 VLAN。

**答案：**

**【问题 1】** 通过把工程部的用户放到他(或她)自己的基于 MAC 地址的 VLAN 中。这个 VLAN 所惟一允许的访问，只有该用户自己。任何其他用户都不能监听到该用户的内容，因为该用户的内容不会转发到其他的网段上去。另外，还有一种更加安全的方式，分配一个专用的端口给这个用户，为他或她产生一个基于端口的 VLAN。

**【问题 2】** 产生一个基于 IP 子网的 VLAN，使用 IP 地址来表示用户。这样无论用户处在何处都能进行网络访问。

**【问题 3】** 产生一个组播地址的 VLAN。

**【问题 4】** 产生一个基于 MAC 地址的 VLAN，使公司总裁成为其他各部门的 VLAN 的成员。



例4 阅读以下说明,回答问题。

【说明】某单位现有的网络是基于传统路由器作为主干设备的,实现了 LAN 子网的隔离和连接,但随着业务的增加及多媒体的应用,该网络运行的越来越慢。

【问题1】简述传统路由器对网络造成的主要限制。

【问题2】如何对网络进行改进。

分析:和传统的路由器相比,三层交换机的路由速度一般要快十倍或数十倍,能实现线速路由转发。传统路由器采用软件来维护路由表,而三层交换机采用专用的芯片硬件来维护路由表,因而能实现线速的路由。

在局域网上,二层的交换机通过源 MAC 地址来标识数据包的发送者,根据目的 MAC 地址来转发数据包。对于一个目的地址不在本局域网上的数据包,二层交换机不可能直接把它送到目的地,需要通过路由设备(比如传统的路由器)来转发,这时就要把交换机连接到路由设备上。

如果把交换机的默认网关设置为路由设备的 IP 地址,交换机会把需要经过路由转发的包送到路由设备上。路由设备检查数据包的目的地址和自己的路由表,如果在路由表中找到转发路径,路由设备把该数据包转发到其他的网段上,否则,丢弃该数据包。

专用(传统)路由器昂贵、复杂、速度慢,易成为网络瓶颈,因为它要分析所有的广播包并转发其中的一部分,还要和其他的路由器交换路由信息,而且这些处理过程都是由 CPU 来处理的(不是专用的芯片硬件),所以速度慢。

三层交换机既能像二层交换机那样通过 MAC 地址来标识转发数据包,也能像传统路由器那样在两个网段之间进行路由转发。而且由于是通过专用的芯片来处理路由转发,三层交换机能实现线速路由。

与传统的路由器相比,三层交换机不仅路由速度快,而且配置简单。在最简单的情况(即第三层交换机默认启动自动发现功能时),一旦交换机接进网络,只要设置完 VLAN,并为每个 VLAN 设置一个路由接口。三层交换机就会自动把子网内部的数据流限定在子网之内,并通过路由实现子网之间的数据包交换。

管理员也可以手工配置路由的方式:设置基于端口的 VLAN,给每个 VLAN 配上 IP 地址和子网掩码,就产生了一个路由接口。随后,手工设置静态路由或者启动动态路由协议。

答案:

【问题1】传统路由器是一个转发并遗忘的网络设备。仅就路由器对任何数据包都要有一个“拆打”过程来看,即使是同一源地址向同一目的地址发出的所有数据包,也要重复相同的过程。这导致路由器不可能具有很高的吞吐量,这也是路由器成为网络瓶颈的原因之一。另外,当流经路由器的流量超过其吞吐量时,将引起路由器内部的拥塞。持续拥塞不仅会使转发的数据包被延误,更严重的是使流经路由器的数据包丢失。再者,路由器的复杂性还对网络的维护工作造成沉重的负担。

【问题2】此系统的瓶颈在于作为主干设备的传统路由器,将其换成具有快速 IP 报文转发的三层交换机,其系统图如图 1.31 所示。

其中高性能三层交换机克服了传统路由器作为 LAN 主干带来的瓶颈问题,使 IP 报文转发接近或达到线速,且对 VLAN 划分以及互联等功能都优于传统路由器。

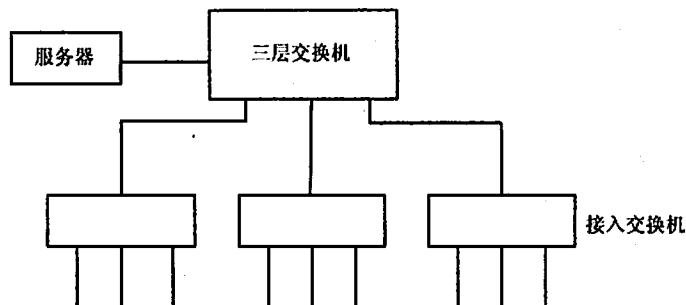


图 1.31 三层交换网络结构图

例 5 阅读以下说明，回答问题。

【说明】在一幢 11 层的大楼内组建一个局域网，该局域网的连接示意图如图 1.32 所示。

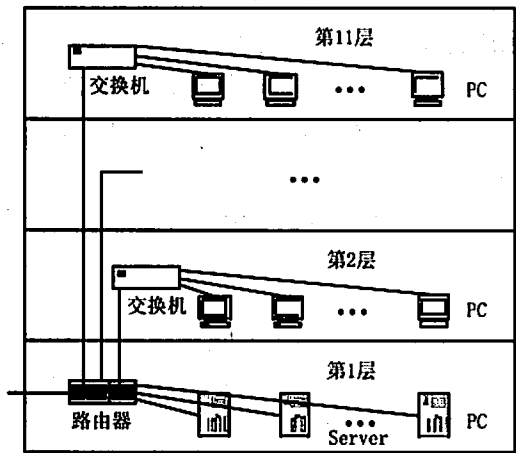


图 1.32 某局域网拓扑图

【问题 1】指出上述解决方案存在什么问题?需要增加什么设备?如何连接?

【问题 2】若在该局域网实现 VLAN，路由器将起什么作用?

分析：通过图 1.32 可看出所有主干所有的交换机与路由器相连，路由器无此功能，一般的做法是各楼层交换机与一台高性能的主交换机相连，主交换机与路由器相连，路由器与 Internet 相连，实现局域网内用户访问互联网。

答案：

【问题 1】这种方案的问题是：缺少主交换设备。解决方法是加入一台主交换机。连接的方法为：各楼层交换机分别连接到主交换机，服务器均连接到主交换机，主交换机连接到路由器。如图 1.33 所示。

【问题 2】VLAN 的主要特征是每个 VLAN 代表一个广播域。路由器的作用就是在各个 VLAN 之间进行数据转发。



例6 阅读以下说明，回答问题。

【说明】用三层交换和千兆位以太网技术，将三个相距大于550m的中心节点连起来，每个中心节点都有财务、人事和教务三类应用并且人员办公位置不固定。客户端机器与中心节点间的距离均小于100m。按应用将全网划分为3个VLAN，三个中心都必须支持3个VLAN的数据转发。请设计一个满足上述需求的园区主干网，具体要求如下：

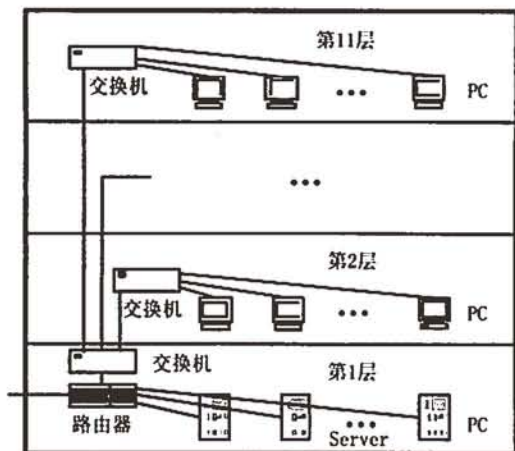


图 1.33 局域网拓扑结构图

【问题1】画出园区主干网的网络拓扑结构图。

【问题2】在图中标出所选用的网络设备和传输介质的名称(如：三层交换机、多模光纤)，并画出VLAN的划分(每个VLAN写明其VLAN号和应用类型，如VLAN 1 财务)。

【问题3】说明所选用的VLAN划分方法。

【问题4】说明对网络设备之间传输VLAN信息的要求。

分析：该网络采用千兆位以太网技术，每个中心节点间用多模光纤通过交换机千兆光纤端口与三层中心交换机千兆光纤端口相连，实现主干之间的千兆互联。VLAN的划分为基于端口划分的VLAN、基于MAC地址划分的VLAN、基于网络层协议划分的VLAN、根据IP组播划分的VLAN。

三层交换机及二级交换机都支持VLAN的划分，同时三层交换机可实现VLAN之间的相互访问。

答案：

【问题1】、【问题2】的答案见图1.34所示。

【问题3】按MAC地址划分VLAN。由网管人员指定属于同一个VLAN中的各客户端机器的MAC地址。

【问题4】将相互之间访问多的机器划分为一个VLAN，如按部门划分VLAN，此目的一是增强安全性，控制VLAN之间的相互访问，二是减少VLAN之间的数据传输量，加快数据传输速率，同一个VLAN内的报文直接在交换设备间进行高速传输，无须经过三层路由。

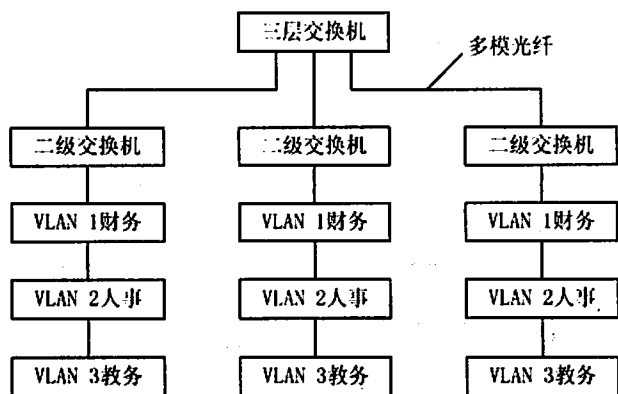


图 1.34 VLAN 划分拓扑结构图

### 1.4.3 同步练习

1. 某网络的连接如图 1.35 所示。

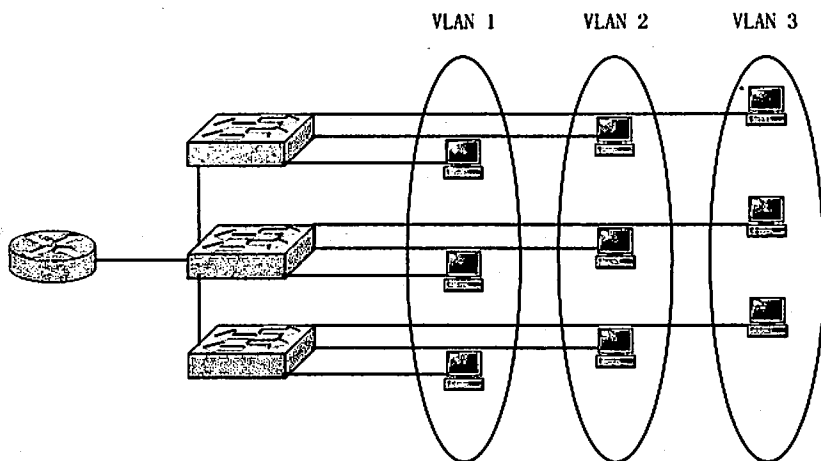


图 1.35 VLAN 示意图

【问题 1】VLAN 技术的核心是什么？

【问题 2】1996 年 IEEE 颁布了用以标准化 VLAN 实现方案的什么协议标准？

【问题 3】VLAN 的分类？

【问题 4】VLAN 工作在 ISO/OSI 参考模型的哪一层？

【问题 5】路由器的作用？

【问题 6】若不采用路由器，全部采用交换机实现，是否可行？给出解释。

2. 三层交换技术不是一种标准化技术，目前广泛应用的三层交换技术有 3COM 的 Fast IP、3COM 的 FIRE、Cisco 的 NetFlow、Cisco 的标记交换。请简要回答下列问题：

【问题 1】能完成 VLAN 之间数据传递的设备是什么？

【问题 2】采用“一次路由，随后交换”方式的三层交换技术是什么？

【问题 3】FastIP 的主要技术基础是什么？

【问题 4】3COM 公司的 FIRE 交换机达到高性能交换是通过什么硬件以线速度来

实现路由器的路由/转发等功能?

【问题5】Cisco 的 NetFlow 技术方案的目的是什么?

#### 1.4.4 同步练习参考答案

1.

【问题1】VLAN 技术的核心是通过路由和交换设备在网络的物理拓扑结构基础上建立一个逻辑网络,以使得网络中任意几个 LAN 段(和)单站能够组合成一个逻辑上的局域网。

【问题2】802.1Q

【问题3】VLAN 的分类有:基于端口的 VLAN、基于 MAC 地址划分的 VLAN、基于网络层协议划分的 VLAN、根据 IP 组播划分的 VLAN。

【问题4】VLAN 工作在 ISO/OSI 参考模型第三层。

【问题5】路由器的作用就是在各个 VLAN 之间进行数据转发。

【问题6】可以,一台交换机具有路由模块(或支持三层交换),作为中心交换机。

2.

【问题1】路由器

【问题2】3COM 的 Fast IP

【问题3】NHRP

【问题4】FIRE 硬件

【问题5】Cisco 的 NetFlow 技术方案的目的是提高路由/转发能力即路由器的性能。

### 1.5 本章小结

这部分内容主要要求考生了解局域网组网设计的原则、组网步骤,掌握局域网的组网技术、以太网交换机的部署、配置和管理、VLAN 的划分。

要求考生综合上述知识,根据用户需求,合理利用局域网设备和技术设计出符合用户需求的网络。

### 1.6 达标训练题及参考答案

#### 1.6.1 达标训练题

1. 请简要回答局域网互联设备的问题。

【问题1】请填写表 1.3 中(1)~(5)处的内容。

【问题2】双绞线、同轴电缆各自应用在什么场合?

【问题3】集线器、网桥、交换机、路由器分别应用在什么场合?它们之间有何区别?

【问题4】假设一个单位的 Hub 是 10BaseT 接口,连在该 Hub 上的计算机设备采用的网卡是 100BaseT 的,那么这个 LAN 能正常工作吗?从该 Hub 到这台计算机设备之间的网

络带宽最大是多少?

表 1.3 网络设备在 OSI 参考模型中的工作位置

网络设备	工作于 OSI 参考模型的哪层
中继器	(1)
集线器	(2)
二层交换机	(3)
三层交换机	(4)
路由器	(5)

2. 假设光速  $C=3 \times 10^8 \text{m/s}$ , 物理层延迟  $t_{\text{PHY}}=0.15 \times 10^{-5} \text{s}$ , 电信号在电缆中的传播速度为  $0.7C$ , 最小帧长  $L_{\text{min}}=512$  字节。有一个中继器, 时延为  $0.15 \times 10^{-5} \text{s}$ , 请计算快速以太网网络系统跨距的近似值。

3. 简要回答下列关于局域网的问题。

【问题 1】画出局域网 OSI 体系结构图。

【问题 2】以太网标准系列中几个主要标准。

【问题 3】分别画出双绞线在网卡与集线器、集线器之间的连接示意图。

4. 阅读以下说明, 回答问题。

【说明】(1)某公司 A 楼为四层, 同一楼层内任意两个房间最远传输距离不超过 90m, A 楼与 B 楼之间距离不超过 500m。网络中心设在 A 楼的三楼, 中心交换机使用三层交换机。B 楼为三层, 接入交换机设于二楼配线间。A 楼与 B 楼其他各层均设置一个配线间, 并且每层楼每个房间至配线间的距离小于 90m。

(2) 公司为保证信息安全, 根据部门划分了多个 VLAN, 每个部门形成一个虚拟局域网。

【问题 1】考虑性能价格因素, 楼层内交换机采用什么传输介质相连, 各信息点采用什么传输介质。

【问题 2】A 楼与 B 楼之间采用什么传输介质。

【问题 3】什么是三层交换技术?

【问题 4】VLAN 有几种分类?

【问题 5】虚拟局域网是怎样增加网络安全性的?

【问题 6】列举出三层交换技术(至少 3 种以上)?

【问题 7】如公司通过 DDN 专线接入互联网, 需要增加什么设备?

【问题 8】根据上述需求, 简单画出网络拓扑结构图。

5. 阅读以下说明, 回答问题。

【说明】某家庭有两台计算机, 该用户申请了 ISDN 专线接入 Internet, 两台计算机均安装了 Windows 2000 操作系统, 其中一台计算机(ISDN 卡和网卡)安装了代理服务软件, 从而保证了另一台计算机通过代理访问 Internet, 其连接示意图所图 1.36 所示。

请回答下列问题:

【问题 1】ISDN 是指什么?

【问题 2】基本速率 ISDN 线路采用的传输为电话铜质双绞线, 包括两个 B 信道, 每



个信道可以传输的数据速率?

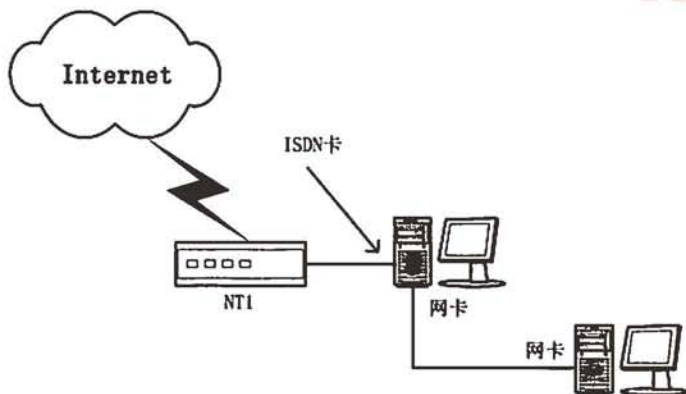


图 1.36 第 5 题连接示意图

【问题 3】画出网卡与网卡之间通过 RJ-45 连接器连接的示意图(要求: 注明每个信号线的序号)。

6. 图 1.37 是某一主干网络拓扑图, 该网络采用千兆三层交换技术。其中(1)、(2)设备位于一幢楼内的主配线间, 网络中心设于该楼, (3)、(4)、(5)、(6)分别位于 4 幢楼内, 楼与楼距离为 2.5km。

请标出联网设备和链路, 并注明设备名称、速率及媒体名称。

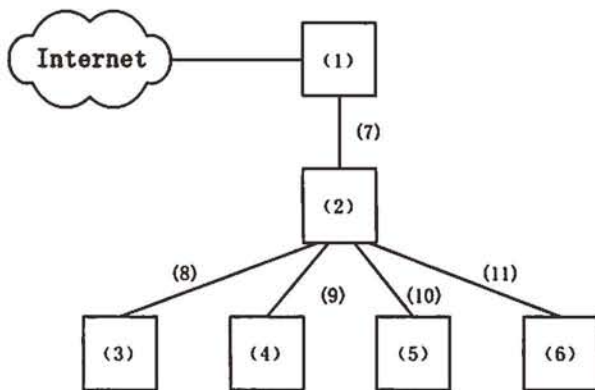


图 1.37 第 3 题连接示意图

## 1.6.2 参考答案

1.

- 【问题 1】(1) 第一层(物理层)      (2) 第一层(物理层)  
(3) 第二层(数据链路层)      (4) 第三层(路由层)  
(5) 第三层(路由层)

【问题 2】双绞线主要应用于星型网络; 同轴电缆用于总线型网络; 双绞线应用于对传输距离、速度、抗噪要求不高的环境。同轴电缆应用于要求具有高带宽和极好的噪声抑制的环境。

【问题 3】集线器是连接网络的重要、常用的设备，主要用于将服务器与工作站连接到网络上，它是星型网络拓扑中常用的设备，在局域网中最为常见。

网桥主要应用于局域网之间的连接，它可以将不同拓扑结构的局域网连接在一起，如总线型网、环型网、星型网的互联。网桥也可以将一个局域网分成不同的网段。网桥的主要作用包括互联、网络寻址、网段隔离、负载均衡和数据转发。

交换机有二层交换机和三层交换机，二层交换机工作在数据链路层，二层交换机主要查看传输的帧内的 MAC 地址，如果知道目的地址，就将信息发送给相应的接口；三层交换机工作在路由层，主要实现路由功能。

路由器是典型的网络层设备，路由器具有判断网络地址和选择路径的功能。常用于异种网络的互联。

【问题 4】10BaseT 表示带宽可以到 10Mb/s，100BaseT 表示带宽可以到 100Mb/s。100BaseT 的网卡是 10M/100M 自适应的，因此该环境可以工作。但是该 Hub 到计算机设备提供的最高带宽是 10Mb/s。

$$2. \text{ slot time} \approx 2S/0.7C + 2t_{\text{min}} + 2N \times \text{tr}$$

$$L_{\text{min}}/R = \text{slot time}$$

$$S \approx 0.35C \times (L_{\text{min}}/R - 2t_{\text{min}} - 2N \times \text{tr})$$

$$\approx 0.35 \times 3 \times 10^8 \times (512/10^8 - 2 \times 0.15 \times 10^{-5} - 2 \times 0.15 \times 10^{-5})$$

$$\approx 117.6(\text{m})$$

网络跨距约为 117.6m。

3.

【问题 1】局域网 OSI 体系结构图如图 1.38 所示。

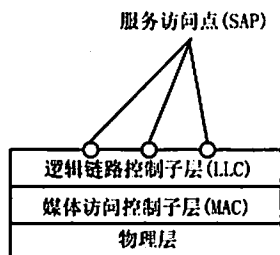


图 1.38 IEEE 802 参考模型

【问题 2】10Base5、10Base 2、10Base T、10BaseF、100BaseTX、100BaseT4、100BaseFX、1000BaseLX、1000BaseSX、1000BaseCX、1000BaseT。

【问题 3】双绞线在网卡与集线器、集线器之间的连接示意图如图 1.39 所示。

4.

【问题 1】楼层内交换机采用双绞线相连，各信息点采用双绞线相连。

【问题 2】A 楼与 B 楼之间采用多模光纤。

【问题 3】三层交换，又称多层交换或 IP 交换，是将传统交换机与传统路由器结合起来的网络设备，它即可以完成传统交换机的端口交换功能，又可以完成部分路由器的路由功能。简单地说，三层交换技术就是：“二层交换技术+三层转发技术”。

【问题 4】VLAN 分类有：基于端口划分的 VLAN、基于 MAC 地址划分的 VLAN、基

于网络层协议划分的 VLAN、根据 IP 组播划分的 VLAN。

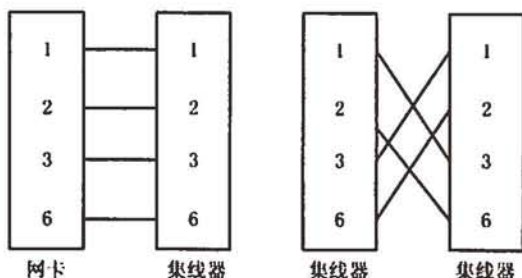


图 1.39 网卡与集线器、集线器之间的连接示意图

【问题 5】虚拟局域网增加网络安全性的方法：

(1) 增强网络安全性的一种最有效和最易管理的方法是将整个网络划分成一个互相独立的广播组(VLAN)。

(2) 网管人员可限制某个 VLAN 中的用户数量，并且可以禁止那些没有得到许可的用户加入到某个 VLAN 中。

(3) 按以上方式，VLAN 可以提供一道安全性防火墙，以控制用户对于网络资源的访问，控制广播组的大小和构成，并且可借助于网管软件在发生非法入侵时及时通知管理人员。

【问题 6】广泛应用的三层交换技术有 3COM 的 Fast IP、3COM 的 FIRE、Cisco 的 NetFlow、Cisco 的标记交换。

【问题 7】如公司通过 DDN 专线接入互联网，需要增加 DDN 专线、路由器等设备。

【问题 8】网络拓扑结构图如图 1.40 所示。

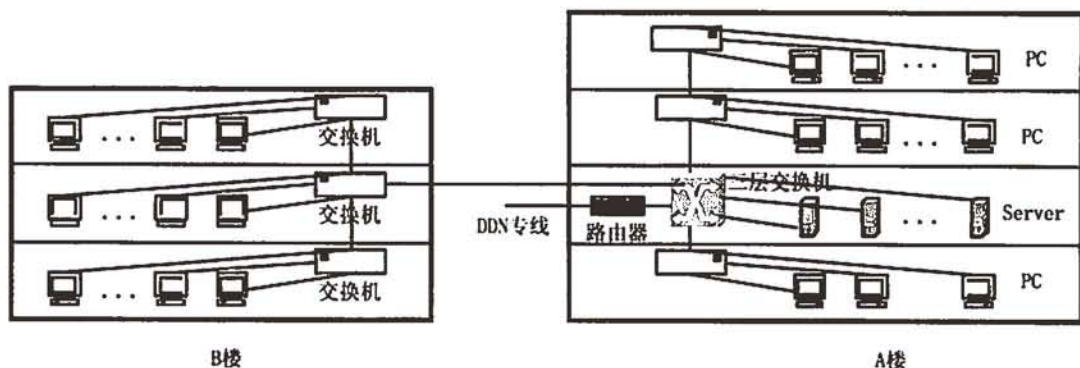


图 1.40 网络拓扑结构图

5.

【问题 1】ISDN 是指综合业务数字网

【问题 2】64Kb/s

【问题 3】网卡与网卡之间通过 RJ-45 连接器连接的示意图如图 1.41 所示。

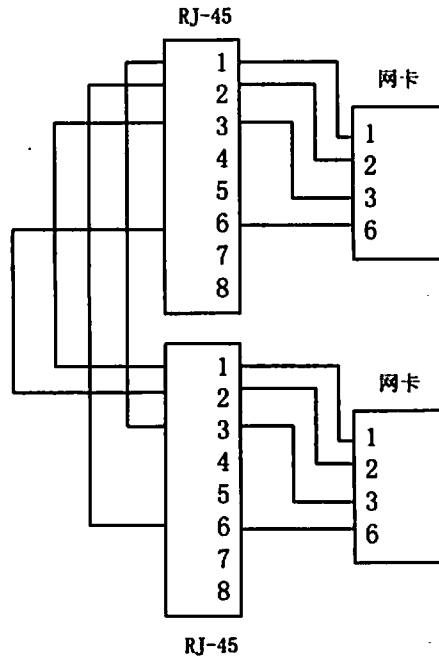


图 1.41 网卡与网卡之间通过 RJ-45 连接器连接的示意图

6. (1)路由器 (2)千兆三层核心交换机  
 (3)(4)(5)(6)千兆二层接入交换机 (7)超五类双绞线  
 (8)(9)(10)(11)单模光纤



## 第2章 综合布线

大纲要求:

- 综合布线概念、组成、设计及依据的标准
- 综合布线基础环境准备
- 线缆及相关硬件的选择与安装
- 综合布线系统的性能指标及测试流程

### 2.1 综合布线

#### 2.1.1 考点辅导

##### 2.1.1.1 综合布线系统概述

###### 1. 什么是综合布线系统

综合布线系统(PDS)是专为通信与计算机网络而设计的,它可以满足各种通信与计算机信息传输的要求,是为具有综合业务需求的计算机数据网开发的。

综合布线系统具体的应用对象主要是通信和数据交换,即语音、数据、传真、图像信号。综合布线系统是一套综合系统,它可以使用相同的线缆、配线端子板、插头及模块插孔,解决传统布线存在的兼容性问题。综合布线系统是智能化大厦工程的重要组成部分,是智能化大厦传送信息的神经中枢。

###### 2. 综合布线系统的特点

与传统布线系统比较,综合布线系统具有兼容性、开放性、灵活性、可靠性、经济性、先进性。

###### (1) 兼容性

兼容性是指其设备可以用于多种系统。它将语音、数据信号的配线统一设计规划,采用统一的传输线、信息插接件等,把不同信号综合到一套标准布线系统中,同时,该系统比传统布线系统简捷很多,不存在重复投资,可以节约大量资金。

###### (2) 开放性

综合布线系统由于采用开放式体系结构,符合国际标准,对现有著名厂商的硬件设备均是开放的,对通信协议也同样是开放的。

###### (3) 灵活性

综合布线系统中每条线路均可传送语音、传真和数据,所有系统内的设备(计算机、终端、网络集散器、集线器或中心集线器、电话、传真)的开通及变动无须改变布线,只要在设备间或管理间作相应的跳线操作即可。

#### (4) 可靠性

综合布线系统全部使用物理星型拓扑结构,任何一条线路有故障都不会影响其他线路,从而提高了可靠性。各系统采用同一传输介质,互为备用,又提高了备用冗余。

#### (5) 经济性

综合布线系统设计信息点时要求按规划容量留有适当的发展容量,因此,就整体布线系统而言,按规划设计所做的经济分析表明,综合布线系统会比传统布线系统的性价比更优,后期运行维护及管理费也会下降。

#### (6) 先进性

综合布线系统为了适应数据传递、语音及多媒体技术的发展采用双绞线与光纤混合布置方式进行布线。

### 3. 综合布线标准

综合布线标准有:

《建筑与建筑群综合布线系统工程设计规范》(国家标准 GB 30511—2000)

《建筑与建筑群综合布线系统工程施工和验收规范》(国家标准 GB 30512—2000)

《大楼通信综合布线系统第一部分总规范》(YD/T 926.1—2001)

《大楼通信综合布线系统第二部分综合布线用电缆光纤技术要求》(YD/T 926.2—2001)

《大楼通信综合布线系统第三部分综合布线用连接硬件技术要求》(YD/T 926.3—2001)

《商用建筑通信布线标准》(北美标准 ANSI/TIA/EIA 568B)

《信息技术——用户通用布线系统》(第二版)(国际标准 ISO/IEC 11801)

《国际电子电气工程师协会:CSMA/CD 接口方法》(IEEE 802.3)

### 4. 综合布线系统的构成

综合布线系统由 6 个子系统组成,即建筑群子系统、设备间子系统、垂直子系统、管理子系统、水平子系统、工作区子系统。大型布线系统需要用铜介质和光纤介质将 6 个子系统集成在一起。

(1) 水平子系统:由信息插座、配线电缆或光纤、配线设备和跳线等组成,又称为配线子系统。

(2) 垂直子系统:由配线设备、干线电缆或光纤、跳线等组成,又称为干线子系统。

(3) 工作区子系统:需要设备终端设备的独立区域。

(4) 管理子系统:是针对设备间、交接间、工作区的配线设备、缆线、信息插座等设施进行管理的系统。

(5) 设备间子系统:是安装各种设备的场所,对综合布线而言,还包括安装的配线设备。

(6) 建筑群子系统:由配线设备、建筑物之间的干线电缆或光纤、跳线等组成。

#### 2.1.1.2 综合布线系统设计

##### 1. 系统设计原则

在进行综合布线系统设计时通常应遵循以下原则:

(1) 采用模块化设计,易于在配线上扩充和重新组合。

- (2) 采用星型拓扑结构,从而使系统扩充和故障分析变得十分容易。
- (3) 应满足通信自动化与办公自动化的需要,即满足语音与数据网络的广泛要求。
- (4) 确保任何插座互连主网络,尽量提供多个冗余互连信息点插座。
- (5) 适应各种符合标准的品牌设备互联入网,满足当前和将来网络的要求。
- (6) 电缆的铺设与管理应符合综合布线系统设计的要求。

## 2. 工作区子系统设计

工作区子系统提供从水平子系统的信息插座到用户工作站设备之间的连接,它包括工作站连线、适配器和扩展线等。

一部电话机或一台计算机终端设备的服务面积可按  $8\sim 10\text{m}^2$  设置,也可按用户要求设置。采用标准信息插座,型号为 RJ-45,采用 8 芯连线,全部按标准制造,符合 ISDN 标准。在 RJ-45 插座内不仅可以插入数据通信通用的 RJ-45 接头,也可以插入电话机专用的 RJ-12 插头。

信息插座通常有 3 种安装形式:信息插座安装于地面上、信息插座安装于分隔板上、信息插座安装于墙上。如安装于墙上应放置在距地面 30~50cm 处。

## 3. 水平子系统设计

水平子系统是将垂直子系统线路延伸到用户工作区,由工作区的信息插座、信息插座至楼层配线设备(FD)的配线电缆或光纤、楼层配线设备和跳线等组成。

水平子系统的设计应按以下要求进行:

(1) 水平子系统一般应使用 20 年左右,通常采用管线敷设,这也对双绞线的性能和质量提出了更高的要求。

(2) 进行网络布线时应考虑未来的发展(信息点冗余及网络带宽的需求)。

(3) 水平子系统采用 4 对双绞线,通常在超 5 类和 6 类之间选择,在高速率应用场合宜采用光缆。

(4) 根据整个综合布线系统的要求,应在交换间或设备间的配线设备上连接,以构成电话、数据传输设备并进行管理,配线电缆宜采用双绞线。电缆长度应在 90m 以内。

## 4. 垂直子系统设计

垂直子系统主要用于连接各层配线室,并连接主配线室。

设计要求:

(1) 为安装和固定垂直子系统的电缆,要求建筑物竖井中应立有金属线槽,且每隔两米焊一根粗钢筋。

(2) 竖井中的线槽应和各层配线室之间有金属线槽连通。

(3) 垂直子系统采用的介质大多数为双绞线电缆、光纤。

## 5. 管理子系统设计

管理子系统由交连、互连配线架组成,为连接其他子系统提供手段。

设计要求:

(1) 根据信息点的数量,对于信息点不是很多的楼层,为便于管理,几个楼层可共用一个子配线间,对于有较多信息点的楼层,一个楼层设置一个配线间。

(2) 配线间的位置可选在弱电井附近的房间内。配线室设标准机柜, 用于安装配线架(双绞线、光纤)和计算机网络通信设备。

#### 6. 设备间子系统

设备间子系统(主配线间)由设备间中的电缆、连接器和相关支撑硬件组成, 它把公共系统设备的各种不同设备互连起来。该子系统将中继线交叉连接处和布线交叉处与公共系统设备(如 PBX)连接起来。

设计要求:

(1) 通常主配架设置在程控机房内, 用于垂直干缆和 PABX 的连接, 建议采用 QCBIX 系列配线架, 可充分满足语音通信的要求。

(2) 通常计算机网络主配线架设在网管中心, 使用光纤配线架, 用来端接来自各分配线间的光纤, 并通过光纤跳线和计算机网络中心交换机相连。光纤配线架可直接安装在标准的 19in 机柜内, 用于主干光纤和网络设备的连接, 十分易于管理。

(2) 对设备间的建设应满足一定的要求, 如室温、湿度、地板负重能力、消防、电源及 UPS 等。

#### 7. 建筑群子系统设计

建筑群子系统应由连接各建筑物之间的综合布线缆线、建筑群配线设备(CD)和跳线等组成。

设计要求:

(1) 建筑物之间的缆线宜采用地下管道或电缆沟的铺设方式。

(2) 建筑物群干线电缆、光缆、公用网和专用网电缆、光缆(包括天线馈线)进入建筑物时, 都应设置引入设备, 并在适当位置转换为室内电缆、光纤。引入设备还包括必要的保护装置。引入设备宜单独设置房间, 如条件合适也可与 BD 或 CD 合设。引入设备的安装应符合相关规定。

(3) 建筑群和建筑物的干线电缆、主干光缆布线的交接不应多于两次。

(4) 从楼层配线架(FD)到建筑群配线架(CD)之间只应通过一个建筑物配线架(BD)。

#### 8. 管线设计

综合布线系统中管线设计通常采用两种方案: 装配式槽形电缆桥架、地面线槽走线。

#### 9. 电气防护、接地及防火设计

综合布线系统应根据环境条件选用相应的缆线和配线设备, 或采取防护措施, 并应符合下列规定:

(1) 当综合布线区域内存在干扰或用户对电磁兼容性有较高要求时, 宜采用屏蔽缆线和屏蔽配线设备进行布线, 也可采用光纤系统。采用屏蔽布线系统时, 所有屏蔽层应该保持连续性。

(2) 综合布线系统采用屏蔽措施时, 必须有良好的接地系统。

(3) 当电缆从建筑物外面进入建筑物时, 电缆的金属护套或光纤的金属件均应有良好的接地, 同时要采用过压、过流保护措施, 并符合相关规定。

(4) 根据建筑物的防火等级和对材料的耐火要求, 综合布线应采取相应的措施。



(5) 当综合布线路以上存在干扰源,且不能满足最小净距要求时,宜采用金属管线进行屏蔽。综合布线缆与附近可能产生高平电磁干扰的电动机、电力变压器等电气设备之间应保持必要的间距。墙上铺设的综合布线缆、光纤及管线与其他管线应保持适当的间距。

### 2.1.1.3 综合布线系统的性能指标及测试

#### 1. 双绞线系统的测试元素及标准

##### (1) 连接图

连接图用于显示双绞线的详细情况。连接图测试通常是一个布线系统的最基本测试,因而对于 3~5 类布线系统,都要求连接图测试。

##### (2) 线缆长度

3~5 类布线系统都要求对线缆长度的准确测试。对线缆长度要求如下:基本回路线缆长度不大于 94m(包括测试跳线),通道回路线缆长度不大于 100m(包括设备跳线和快式跳线)。

##### (3) 衰减

由于集肤效应、绝缘损耗、阻抗不匹配、连接电阻等因素,造成信号沿链路传输损失的能量,称之为衰减。衰减是针对“基本回路”/“通道回路”信号损失程度的量度。最坏线对的衰减应小于“基本回路”/“通道回路”允许的最大衰减值。

##### (4) 近端串音(NEXT)衰减

电磁波从一个传输回路(主串回路)串入另一个传输回路(被串回路)的现象称为串音,能量从主串回路串入回路时的衰减称为串音衰减。在 UTP 布线系统中,近端串音为主要的影响因素。布线系统都应通过 NEXT 衰减的测试,而且 NEXT 衰减的测试必须从两个方向进行,也就是双向测试。

##### (5) 回波损耗(RL)

回波损耗(RL)是电缆传输系统的一个重要参数。该参数定义为开始输入给信号传输系统的信号与信号源接收到的反射信号的功率之比。不良连接器、操作不当或不正确的线缆拖拉和安装方式都会使线缆产生变形,从而引起回波损耗问题的发生。

#### 2. 光缆布线系统的测试元素及标准

##### (1) 波长窗口参数。

##### (2) 光缆布线链路的最大衰减限值。

##### (3) 光回波损耗限值。

#### 3. 测试环境

##### (1) 测试条件。

##### (2) 测试温度。

##### (3) 测试仪表。

#### 4. 测试流程

在开始测试之前,应该认真了解布线系统的特点、用途,信息点的分布情况,确定测

试标准, 选定测试仪后按下述程序进行:

- (1) 测试仪测试前自检, 确认仪表是正常的。
- (2) 选择测试了解方式。
- (3) 选择设置线缆类型及测试标准。
- (4) NVP 值核准, 核准 NVP 使用缆长不短于 15m。
- (5) 设置测试环境湿度。
- (6) 根据要求选择【自动测试】或【单项测试】。
- (7) 测试后存储数据并打印。
- (8) 发生问题修复后复测。
- (9) 测试中出现“失败”后查找故障。

### 2.1.2 典型例题分析

**例 1** 综合布线的特点为兼容性、开放性、\_\_\_\_\_、可靠性、经济性、先进性。

**分析:** 传统的布线方式是封闭的, 其体系结构是固定的, 若要迁移设备或增加设备是相当困难而麻烦的, 甚至是不可能的。综合布线采用标准的传输线缆和相关连接硬件, 模块化设计。因此所有通道都是通用的, 每条通道均可传送语音、传真和数据。所有系统内的设备的开通及变动无须改变布线, 只要在设备间或管理间作相应的跳线操作即可, 因此非常灵活方便。

**答案:** 灵活性

**例 2** 综合布线系统的\_\_\_\_\_是由工作区用的信息插座、信息插座至楼层配线设备的配线电缆或光纤、楼层配线设备和跳线等组成。

**分析:** 水平子系统宜采用 4 对双绞电缆, 水平子系统在高速率应用场合, 宜采用光缆。水平子系统电缆长度应在 90m 以内。

**答案:** 水平子系统

**例 3** \_\_\_\_\_是一个能够支持任何用户选择的语音、数据、图形图像的布线系统。

**分析:** 综合布线系统中设备可以用于多种系统。它将语音、数据信号的配线统一设计规划, 采用统一的传输线、信息插件等, 把不同信号综合到一套标准布线系统中。

**答案:** 综合布线系统

**例 4** 为了保证综合布线系统的先进性, 综合布线系统中应采用什么介质进行布线?

**分析:** 随着信息时代的快速发展, 数据传递和语音传递并驾齐驱, 多媒体技术迅速崛起, 如仍采用传统布线, 在技术上过于落后。综合布线系统采用双绞线与光纤混合的布置方式是比较科学和经济的方式。

**答案:** 采用双绞线与光纤介质混合进行布线

**例 5** 综合布线系统的\_\_\_\_\_应由设备间的配线设备和跳线以及设备间至各楼层配

线间的连接电缆组成。

分析：综合布线垂直子系统，主要用于连接各层配线室，并连接主配线室。常用介质为双绞线电缆及光纤。

答案：垂直子系统

例6 在综合布线系统中，(1)传输系统应能满足建筑与建筑群对电话、数据、计算机、电视等的综合传输要求，当用于计算机局域网时，宜采用(2)；作为远距离电信网的一部分时应采用(3)。

分析：当综合布线系统需要在一个建筑群之间铺设较长距离的线路，或者在建筑物内信息系统要求组成高速率网络，或者与外界其他网络特别与电力电缆网络一起铺设有抗电磁干扰要求时，宜采用光缆作为传输媒体。光缆可分为多模光缆和单模光缆两种，应用于不同的环境中。

答案：(1)光缆 (2)多模光缆 (3)单模光缆

例7 在综合布线系统中，为解决兼容性问题，所选用的线缆、配线端子板、插座及模块插孔必须\_\_\_\_\_。

分析：综合布线系统中，将语音、数据信号的配线统一设计规划，采用统一的传输线、信息插座等，把不同信号综合到一套标准布线系统中。

答案：相同

例8 在北京某设计院的一间办公室中某PC机访问其他设备速度非常慢，而连接在同一Hub上的其他PC机相互访问速度正常。利用FLUKE DSP4000 电缆测试仪测试后发现，PC到Hub的链路距离达到361英尺(110m)，伴随着电缆超长，仪器同时报告衰减失败。请分析原因。

分析：这是由于双绞线电缆超距造成的。

答案：由于电缆超长导致信号衰减过大，从而导致信号接收端无法正确识别信号，网络纠错功能要求发送端重新发送数据，如此反复，导致网络访问性能下降。

例9 结构化布线系统是一种模块化且灵活性极高的建筑物内的信息传输系统，其结构主要采用(1)。它一般由六个子系统组成，其中将用户的终端设备连接到布线系统的子系统称为(2)；连接各管理间、设备间的子系统称为(3)；对布线电缆进行端接及配线的子系统称为(4)。(2001年网络程序员上午试卷46~49)

- |                |           |           |           |
|----------------|-----------|-----------|-----------|
| (1) A. 星型      | B. 总线型    | C. 环型     | D. 树型     |
| (2) A. 平面楼层子系统 | B. 设备间子系统 | C. 工作区子系统 | D. 建筑群子系统 |
| (3) A. 管理子系统   | B. 设备间子系统 | C. 干线子系统  | D. 用户端子系统 |
| (4) A. 电源子系统   | B. 垂直竖井系统 | C. 设备间子系统 | D. 管理子系统  |

分析: 综合布线系统是种模块化、灵活性极高的建筑群内的信息传输系统, 也是一种集成化的通用传输系统, 在进行综合布线系统设计时一般采用星型拓扑结构, 使系统扩充和故障分析变得十分简易。

综合布线系统由 6 个子系统组成, 即建筑群子系统、设备间子系统、干线子系统、管理子系统、配线子系统、工作区子系统。大型布线系统需要用铜介质和光纤介质将 6 个子系统集成在一起。如图 2.1 所示。

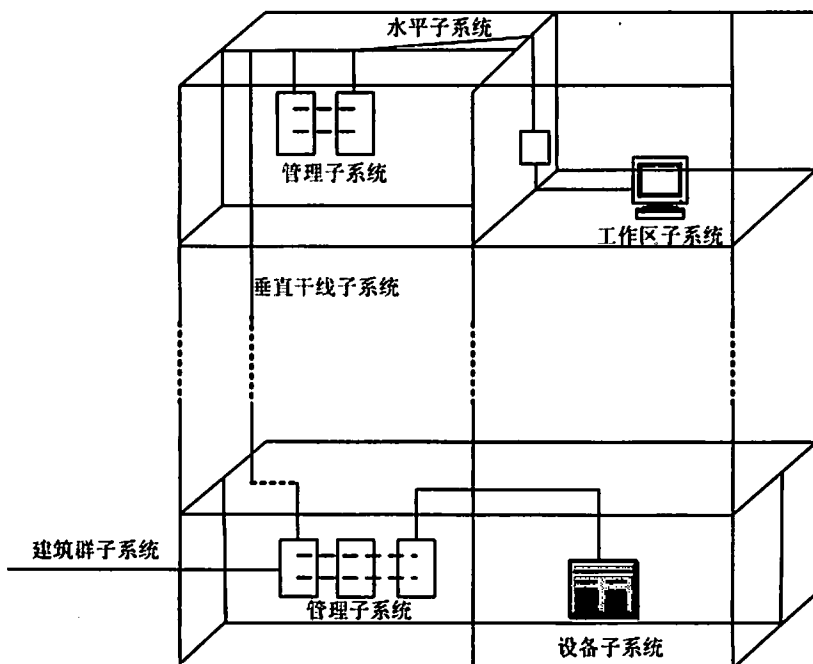


图 2.1 综合布线系统的构成

工作区子系统提供从水平子系统的信息插座到用户工作站设备之间的连接, 它包括工作站连线、适配器和扩展线等。

水平子系统的作用是将垂直干线子系统从配线间延伸到用户工作区, 包括双绞线电缆、信息插座等。

垂直干线子系统是建筑物内网络系统的中樞, 将各楼层的配线间(管理子系统)连到主机房的配线间。

管理子系统就是配线架, 它把水平子系统和垂直干线子系统连在一起, 或把垂直主干和设备子系统连在一起。通过它可以改变布线系统各子系统之间的连接关系, 从而管理网络通信线路。

建筑群子系统将一个园区的各建筑物内的设备子系统连接在一起, 包括光缆、电缆和电气保护设备。

设备间子系统把垂直主干和网络设备连接起来。由设备间中的电缆、连接器和相关支撑硬件组成。



答案: (1)A (2)C (3)C (4)D

**例 10** 结构化布线系统中,所有的水平布线 UTP(非屏蔽双绞线)都是从工作区到各楼层配线间的。在工作区由 (1) 端接,在配线间由 (2) 端接。当布线结构需要调整时,可以通过布线配线系统来重新配置,具体调整手段是通过 (3) 实现。结构化布线工程中常采用 4 对 UTP,它使用 (4) 等四种颜色标识,其对应的 I/O 信息模块有两种标准:即 T568A 和 T568B,它们之间的差别只是 (5)。(2002 年网络程序员上午试卷 56~60)

- |                            |               |
|----------------------------|---------------|
| (1) A. RJ-45 接插头           | B. I/O 信息插座模块 |
| C. 快接式跳线                   | D. 网卡         |
| (2) A. 配线架                 | B. 接插件        |
| C. 干线子系统                   | D. 集线器或交换机    |
| (3) A. 专用工具                | B. 连接块        |
| C. 跳线                      | D. 控制器        |
| (4) A. 橙、蓝、紫、绿             | B. 紫、黑、蓝、绿    |
| C. 黑、蓝、棕、橙                 | D. 橙、绿、蓝、棕    |
| (5) A. “1、2”对线与“3、6”对线位置交换 |               |
| B. “4、5”对线与“7、8”对线位置交换     |               |
| C. “1、2”对线与“4、5”对线位置交换     |               |
| D. “3、6”对线与“7、8”对线位置交换     |               |

**分析:** 综合布线系统是一种集成化的通用传输系统,它利用双绞线或光缆来传输建筑物内的多种信息。SCS 将所有的语音、数据、图像及监控设备的布线组合在一套标准的布线系统上,采用统一的线缆、插头、插座及配线架,当终端机的位置需要变动时,只需将其插入新地点的插座上,然后做一些简单的跳线就行了,不需要再布放新的线缆,也不需要安装新的插孔。另一方面,综合布线采用星型结构,系统的管理维护及故障的检查和排除也非常方便,综合布线以其高度的灵活性及多元化服务而越来越得到人们的重视。

结构化布线可分为 6 个子系统:工作区子系统、水平布线子系统、管理子系统、干线子系统、设备间子系统、建筑群子系统。

结构化综合布线工程中常采用 4 对的 UTP,使用橙、绿、蓝、棕四种颜色标识,而且这些颜色有公认的规定。水晶头的制作很关键,特别是在 100M 的网络中。很多人认为只要线两端的水晶头的次序一样就行,殊不知,5 类双绞线里 4 股线的“绕阻”是不一样的。水晶头的制作有两种常用标准:T568A 和 T568B。制作水晶头时应注意:

(1) 用 Hub 或交换机相互组网时,一根线的两头必须用同一个标准制作。在同一个 Hub 或交换机上最好只用一种标准制作网线。

(2) 当只有两台计算机、不用 Hub 或交换机时,线的一头采用 T568A 标准,另一头采用 T568B 标准。因为,网卡的脚 1 和脚 2 用作发送数据,而脚 3 和脚 6 用作接收数据。两种不同的标准正好将 1、2、3、6 相对应。

(3) 不管两台计算机的物理位置多近,线的长度最好大于 1.5m。不然也会发生时断时续的现象。

答案: (1)B (2)A (3)C (4)D (5)A

例 11 在网络综合布线中,工作区子系统的主要传输介质是\_\_\_\_\_。(2004 年下半年网络管理员上午试卷 44)

A. 单模光纤 B. 5 类 UTP C. 同轴电缆 D. 多模光纤

分析: 工作区子系统提供从水平子系统的信息插座到用户工作站设备之间的连接, 它包括工作站连线、适配器和扩展线等。其中使用的传输介质主要是双绞线。

答案: B

例 12 阅读以下说明, 回答问题。(2004 年下半年网络管理员下午试题一)

【说明】

某公司 A 楼高 40 层, 每层高 3.3m, 同一楼层内任意两个房间最远传输距离不超过 90m, A 楼和 B 楼之间距离为 500 米, 需在整个大楼进行综合布线, 结构如图 2.2 所示。

为满足公司业务发展的需要, 要求为楼内客户机提供数据速率为 100Mb/s 的数据、图像及语音传输服务。

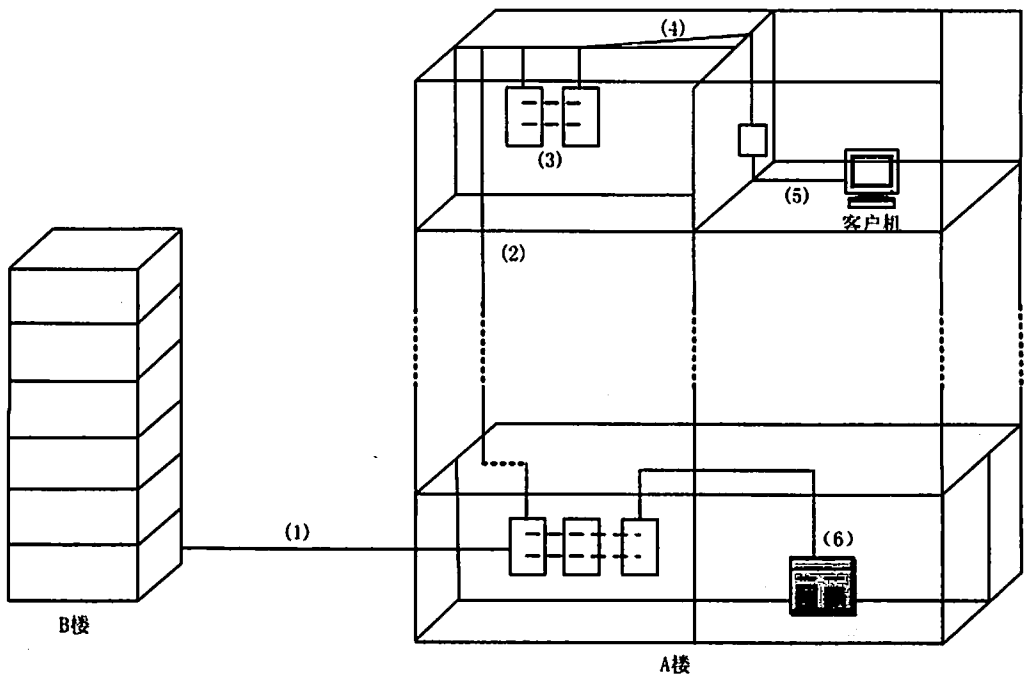


图 2.2 综合布线系统的构成

【问题 1】综合布线系统由 6 个子系统组成, 填写出图 2.2 中(1)~(6)处空缺子系统的名称。

【问题 2】考虑性能与价格因素, 图 2.2 中(1)、(2)和(4)中各应采用什么传输介质?

【问题 3】为满足公司要求, 通常选用什么类型的信息插座?

【问题 4】制作交叉双绞线(一端按 EIA/TIA 568A 线序, 另一端按 EIAFFIA 568B 线序)时, 其中一端的线序如图 2.3(a)所示, 另一端线序如图 2.3(b)所示, 填写出图 2.3(b)中(1)~(8)处空缺的颜色名称。

分析: 结构化布线可分为 6 个子系统: 工作区子系统、水平布线子系统、管理子系统、干线子系统、设备间子系统、建筑群子系统。

随着信息时代的快速发展,数据传递和语音传递并驾齐驱,多媒体技术迅速崛起,如仍采用传统布线,在技术上太落后。综合布线系统采用双绞线与光纤混合的布置方式是比较科学和经济的方式。

综合布线中采用标准信息插座,型号为 RJ-45,采用 8 芯连线,全部按标准制造,符合 ISDN 标准。在 RJ-45 插座内不仅可以插入数据通信通用的 RJ-45 接头,也可以插入电话机专用 RJ-12 插头。

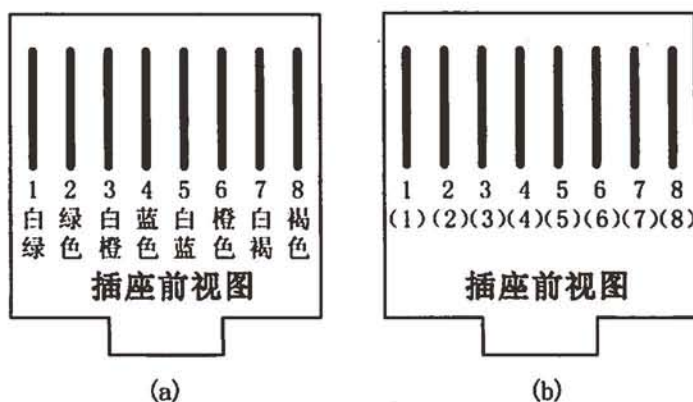


图 2.3 EIA/TIA RJ45 接口线序

双绞线与交叉线的制作遵循 EIA/TIA568 标准。

答案:

【问题 1】

- (1) 建筑群子系统(或户外子系统)
- (2) 干线子系统(或垂直子系统)
- (3) 管理子系统(或布线、跳线子系统)
- (4) 配线子系统(或水平子系统)
- (5) 工作区子系统(或用户端子系统)
- (6) 设备间子系统(或机布线、跳线子系统)

【问题 2】

- (1) 多模光纤
- (2) 多模光纤
- (3) 5 类双绞线(或超 5 类双绞线)

【问题 3】

RJ-45 插座(或信息模块式超 5 类信息插座、多媒体信息模块式超 5 类信息插座)

【问题 4】

- (1) 白橙(2)橙色(3)白绿(4)蓝色
- (5) 白蓝(6)绿色(7)白褐(8)褐色

### 2.1.3 同步练习

1. 综合布线系统与传统的布线系统的最大区别在于:综合布线系统与当前所连接的设

备位置\_\_\_\_\_。

2. 传统的布线方式是 (1) 的。其体系结构是 (2) , 若要迁移设备或增加设备是相当困难而麻烦的, 甚至是不可能的。

3. 综合布线的首要特点是它的 (1) 。所谓 (2) , 将语音、 (3) 的配线统一设计规划, 采用统一的传输线、信息插座等, 把不同信号综合到一套标准布线系统中。由此可见, 这种布线方式比传统布线方式简捷很多, 不存在重复投资, 可以节约大量资金。

4. 综合布线系统采用屏蔽措施时, 必须有良好的接地系统, 单独设置接地体时, 保护地线的接地电阻不应大于 (1) ; 采用接地体时, 不应大于 (2) ; 若接地系统中存在两个不同的接地体时, 其接地电位不应大于 (3) 。

5. 综合布线系统, 最关键的问题是\_\_\_\_\_。

6. 局域网中常用的双绞线为 3 类、4 类和 5 类, 为适应网络速度的不断提高, 近年又出现了超 5 类和 6 类双绞线, 其中\_\_\_\_\_双绞线可满足最新的千兆以太网应用。

7. 在综合布线系统中, 当布线系统需要调整时, 可以通过\_\_\_\_\_来重新配制系统。

8. 有几栋建筑物, 周围还有其他电力电缆, 若需将该几栋建筑物连接起来构成骨干型园区网, 则采用\_\_\_\_\_比较合适。

9. 对双绞线系统进行测试时, 要求通道回路总长度为 (1)m 以内; 基本回路总长度为 (2)m 以内。

10. 综合布线系统在布线施工工程中应遵循哪些标准?

11. 综合布线系统中管线设计通常采用哪些方案?

12. 在综合布线系统测试中对测试仪表有哪些要求?

## 2.1.4 同步练习参考答案

1. 无关

2. (1)封闭 (2)固定

3. (1)兼容性 (2)兼容性 (3)数据信号

4. (1)4  $\Omega$  (2)1  $\Omega$  (3)1Vr.m.s

5. 灵活性和使用寿命

6. 6 类

7. 跳线

8. 光缆

9. (1)100 (2)94

10. 布线施工工程应遵循布线测试、安装、管理、防火、机房及防雷接地等标准。

11. 综合布线系统中管线设计通常采用装配式槽形电缆桥架与地面线槽走线两种方案。

12. 按时域原理设计的测试仪均可用于综合布线现场测试, 但测试仪的测量扫描步长要满足近端串扰指标测量精度的基本保证, 能够在 0~250MHz 频率范围内提供各测试参数的标称值和阈值曲线, 每测试一条链路时间不应大于 25s, 且每条链路应具有一定的故障定位诊断能力, 具有自动、连续、单项选择测试的功能。



## 2.2 本章小结

这部分内容主要要求考生认识综合布线系统的基本概念，综合布线系统的设计，综合布线系统的传输介质以及综合布线系统的性能及其测试。

## 2.3 达标训练题及参考答案

### 2.3.1 达标训练题

1. 什么是综合布线？综合布线的特点是什么？综合布线系统由哪几个子系统构成？
2. 在综合布线中，对双绞线进行测试，主要测试哪些元素？
3. 在综合布线中，对光纤进行测试，主要测试哪些元素？

### 2.3.2 参考答案

1. 综合布线系统(PDS)是专为通信与计算机网络而设计的，它可以满足各种通信与计算机信息传输的要求，是为具有综合业务需求的计算机数据网开发的。

与传统布线系统比较，综合布线系统具有兼容性、开放性、灵活性、可靠性、经济性、先进性的特点。

综合布线系统由6个子系统组成，即建筑群子系统、设备间子系统、干线子系统、管理子系统、配线子系统、工作区子系统。

2. 连接图、线缆长度、衰减、近端串音衰减、回波损耗。
3. 波长窗口、衰减、回波损耗。

# 第 3 章 小型计算机局域网服务器配置

大纲要求:

- IP 地址、子网掩码的规划配置
- DNS 服务器的规划、设置和维护(Linux 环境和 Windows 环境)
- 电子邮件服务器的规划、设置和维护(Linux 环境和 Windows 环境)
- FTP 服务器的规划、设置和维护(Linux 环境和 Windows 环境)
- 代理服务器的规划、设置和维护(Linux 环境和 Windows 环境)
- DHCP 服务器的安装与设置

## 3.1 IP 地址及其规划

### 3.1.1 考点辅导

#### 3.1.1.1 IP 地址基础

Internet 是由不同物理网络互联而成的, 不同网络之间实现计算机的相互通信必须有相应的地址标识, 这个地址标识称为 IP 地址如图 3.1 为 IP 地址的组成与表示。

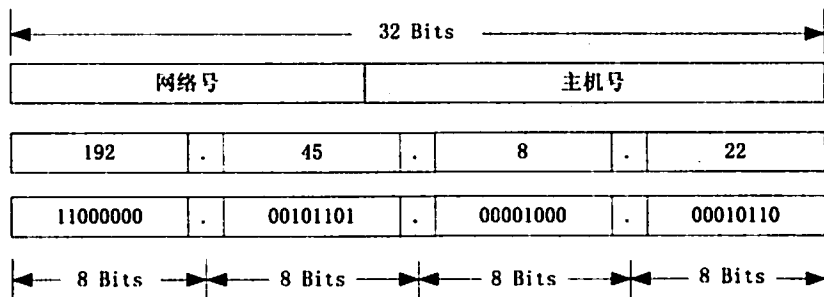


图 3.1 IP 地址的组成与表示

#### 1. IP 地址的组成

一个 IP 地址由网络号和主机号两部分组成。同一个物理网络上的所有主机都用同一个网络号, 网络上的一个主机(包括网络上的工作站、服务器和路由器等)有一个主机号与其对应。据此把 IP 地址划分为两个部分, 一部分用以标明具体的网络段, 即网络号(net-id); 另一部分用以标明具体的节点, 即主机号(host-id)。

#### 2. IP 地址表示

一个 IP 地址由 4 个字节共 32 位的数字串组成, 这 4 个字节通常用小数点分隔。每个字节可用十进制表示, 如 192.45.8.22。IP 地址也可以用二进制和十六进制表示。

### 3. IP 地址的分类

IP 协议的寻址方式支持 5 种不同的网络类型：A 类、B 类、C 类、D 类和 E 类。其中，A、B、C 类地址是基本的 Internet 地址，是用户使用的地址。D 类地址被称为组播地址（多点播送地址），而 E 类地址尚未使用，以保留给将来使用。IP 地址的最左边的 1 个或多个二进制位通常用来指定网络的类型。例如，A 类地址的第一位为“0”，B 类地址的前两位为“10”，C 类地址的前三位为“110”。图 3.2 和表 3.1 说明 5 种不同网络类型 IP 地址的特征和地址容量。

	0	1	2	3	4	7 8	15 16	23 24	31		
A 类地址:	0	网络号					主机号				
B 类地址:	1	0	网络号					主机号			
C 类地址:	1	1	0	网络号					主机号		
D 类地址:	1	1	1	0	组播地址						
E 类地址:	1	1	1	1	0	保留给试验使用					

图 3.2 IP 地址的分类

**A 类：**一个 A 类 IP 地址由 1 个字节的网络地址和 3 个字节的主机地址组成，网络地址的最高位必须是“0”（每个字节有 8 位二进制数）。8 位作为网络号，24 位作为主机号，最多可以表示 126 个网络号（0 和 127 用作特殊地址），每个 A 类地址主机数最多可有  $2^{24}-2$  (16777214) 个。

**B 类：**一个 B 类 IP 地址由 2 个字节的网络地址和 2 个字节的主机地址组成，网络地址的最高两位必须是“10”。16 位作为网络号，16 位作为主机号，最多可以表示  $2^{14}$  (16384) 个网络号，每个 B 类地址主机数最多可有  $2^{16}-2$  (65534) 个。

**C 类：**一个 C 类地址是由 3 个字节的网络地址和 1 个字节的主机地址组成，网络地址的最高三位必须是“110”。24 位作为网络号，8 位作为主机号。共有  $2^{21}$  (2097152) 个网络号，每个 C 类地址主机数不超过  $2^8-2$  (254) 个。

**D 类：**用于多点播送。第一个字节以“1110”开始。因此，任何第一个字节大于 223 小于 240 的 IP 地址是组播地址。

**E 类：**以“11110”开始，保留给试验使用的地址。

表 3.1 Internet 的 IP 地址空间容量

IP 地址类型	第一字节 十进制范围	二进制固定 最高位	二进制 网络位	网络数	二进制 主机位	主机数
A 类	0~127	0	8 位	126	24 位	16777214
B 类	128~191	10	16 位	16384	16 位	65534
C 类	192~223	110	24 位	2097152	8 位	254
D 类	224~239	1110	组播地址			
E 类	240~255	11110	保留给试验使用			

4. IP 地址的特殊形式

IP 地址除了可用于标识一台主机外，还有几种用于表示特殊意义的形式，如表 3.2 所示。

表 3.2 一般不使用的特殊 IP 地址

特殊地址	net-id	host-id	源地址使用	目的地址使用
本网络的本台主机	全 0	全 0	可以	不可以
本网络的某个主机	全 0	host-id	不可以	可以
网络地址	net-id	全 0	可以	可以
直接广播地址	net-id	全 1	不可以	可以
受限广播地址	全 1	全 1	不可以	可以
环回地址	127	任何数	可以	可以

(1) 本网络的本台主机：若一个 IP 地址全由 0 组成，即 0.0.0.0，表示在本网络上的本台主机，当一台主机在运行引导程序但又不知道其 IP 地址时使用该地址。

(2) 本网络的某个主机：网络号各位全为“0”的 IP 地址，表示在这个网络中的特定主机。它用于向同网络中其他主机发送报文的主机。

(3) 网络地址：主机号各位全为“0”的 IP 地址，标识本网络的网络地址。

(4) 直接广播地址(有时简称为广播地址)：主机号各位全为“1”的 IP 地址，它用于将一个分组发送给特定网络上的所有主机，即对全网广播。

(5) 受限广播地址：网络号和主机号都为 1 的 IP 地址(即 255.255.255.255)，它也是对当前网络进行广播，多数是用在当一台主机在运行引导程序时，但又不知道其 IP 地址需要向服务器获取 IP，这时用该地址作为目的地址发送分组。

(6) 环回地址(Loopback Address)：A 类网络地址 127.x.x.x 是一个保留地址，用于网络软件测试以及本地进程间的通信。

5. 保留 IP 地址

如果一个组织不需要接入到因特网上，但需要在其网络上运行 TCP/IP 协议，最佳选择是使用保留地址。保留地址不需要从因特网管理机构申请，任何组织都可以使用这些地址。这些地址在一个组织内部是惟一的，但从全局来看却不是惟一的。同时因特网的路由器也不转发目标地址为保留地址的数据包。保留地址如表 3.3 所示。

表 3.3 Internet 的保留 IP 地址空间

类型	网络号	网络数
A 类	10.0.0.0	1
B 类	172.16.0.0 至 172.31.0.0	16
C 类	192.168.0.0 至 192.168.255.0	256



### 3.1.1.2 子网的划分

#### 1. 为什么要划分子网

(1) IP 地址空间利用率很低。由于 Internet 的 IP 地址采用两级结构, 即网络号和主机号, 这样的设计有不够合理的地方。IP 地址中的 A 至 C 类地址, 可供分配的网络号码超过 211 万个, 而这些网络上的主机号的总数则超过 37.2 亿个, 初看起来, 似乎 IP 地址足够全世界来使用(在 20 世纪 70 年代初期设计 IP 地址时就是这样认为的)。其实不然。第一, 当初没有预计到计算机普及得如此之快, 各种局域网以及局域网上的主机数目急剧增长。第二, IP 地址在使用时有很大的浪费。例如: 某个单位申请到了一个 B 类地址, 但该单位只有 1 万台主机。于是, 在一个 B 类地址中的其余 5 万 5 千多个主机号就白白地浪费了, 因为其他单位的主机无法使用这些号码。

(2) 大型的网络将影响网络性能。从网络吞吐量考虑, 将大量主机安装在一个网络上往往会影响网络的性能。当网络上工作的主机数小于一定数值时, 网络的吞吐量和网络上工作的主机数大约成正比。但是当网络上工作的主机数超过一定数量时, 拥塞就可能产生, 这就导致网络的吞吐量增加速度变慢; 甚至反而会随着主机数的增加而下降。

(3) IP 地址的两级结构不够灵活。有时情况紧急, 一个单位需要新的地点马上开通一个新网络。但是在申请到一个新的 IP 地址之前, 新增加的网络不可能连接到因特网上工作。我们希望有一种方法, 使本单位能随时灵活地增加本单位的网络, 而不必事先到因特网管理机构去申请新的网络号。原来的两级 IP 地址结构无法做到这一点。

#### 2. 从两级 IP 地址到三级 IP 地址

为了解决上述问题, 在 IP 地址中又增加了一个“子网号字段”, 使原来两级的 IP 地址变成三级的 IP 地址, 它能够较好地解决上述问题, 并且使用起来也很灵活。划分子网的基本思路如下:

(1) 一个拥有许多物理网络的单位, 可将其物理网络划分为若干个子网(subnet)。划分子网纯属一个单位内部的事情, 本单位以外的网络看不见这个网络由多少子网组成, 对外仍表现为一个没有划分子网的网络。

(2) 划分子网的方法是从网络的主机号借用若干位作为子网号 subnet-id, 而主机号 host-id 也就相应减少了若干位。于是两级的 IP 地址在本单位内部就变为三级 IP 地址: 网络号 net-id、子网号 subnet-id 和主机号 host-id, 如图 3.3 所示。

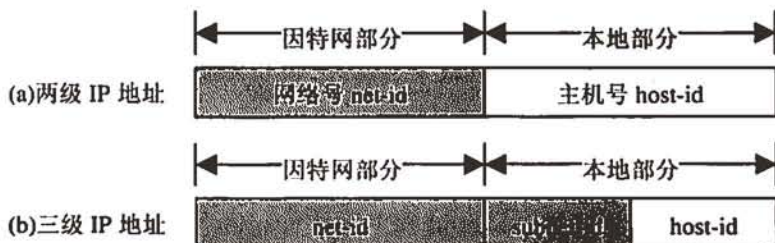


图 3.3 从两级 IP 地址到三级 IP 地址(一)

(3) 凡是从其他网络发送给本单位某个主机的 IP 数据报, 仍然是根据 IP 数据报的目

的网络号 net-id 找到连接在本单位网络上的路由器。但此路由器在收到 IP 数据报后, 再按目的网络号 net-id 和子网号 subnet-id 找到目的子网, 将 IP 数据报交付给目的主机。

下面用一个例子来说明划分子网的概念。图 3.4 表示一个单位拥有一个 B 类 IP 地址, 网络地址是 141.14.0.0(net-id 是 141.14)。凡目的地址为 141.14.x.x 的数据报都被送到这个网络上的路由器 R1。

现将图 3.4 的网络划分为三个子网, 如图 3.5 所示。这里假设子网号 subnet-id 占 8 位, 因此在增加了子网号后, 主机号 host-id 就只有 8 位。所划分的三个子网分别是: 141.14.2.0、141.14.7.0 和 141.14.99.0。在划分子网后, 整个网络对外部仍表现为一个网络, 其网络地址仍然是 141.14.0.0。但路由器 R1 收到数据报后, 再根据数据报的目的地址将其转发到相应的子网。

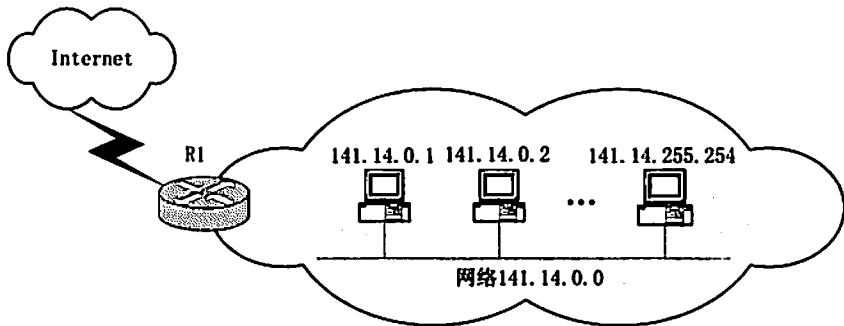


图 3.4 从两级 IP 地址到三级 IP 地址(二)

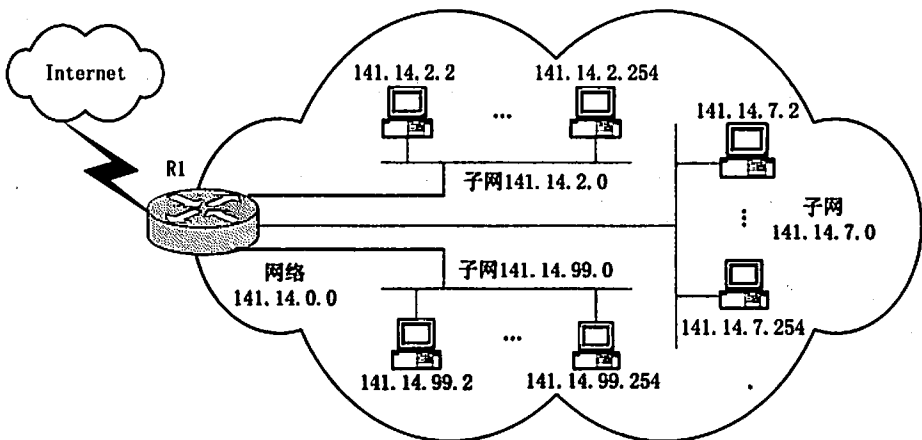


图 3.5 从两级 IP 地址到三级 IP 地址(三)

### 3. 子网掩码

虽然上面已经把—个网络划分成为若干个—子网, 但路由器 R1 必须知道数据报中目的 IP 地址的网络号 net-id、子网号 subnet-id 和主机号 host-id 各是多少位, 这就需要通过子网掩码(Subnet mask)来实现。

子网掩码和 IP 地址—样, 也是 32 位长, 由—串 1 和跟随的—串 0 组成。子网掩码中的 1 对应于 IP 地址中的网络号 net-id 和子网号 subnet-id, 而子网掩码中的 0 对应于 IP 地址

中的主机号 host-id。要得到网络或子网地址,只需将 IP 地址和子网掩码进行按位“与”(AND)运算就可以得到。图 3.6 说明了子网掩码的工作方式。

IP 地址:	141.14.2.21
	10001101 00001110 00000010 00010101
子网掩码:	255.255.0.0
	11111111 11111111 00000000 00000000
网络地址:	141.14.0.0
	10001101 00001110 00000000 00000000

(a) 不划分子网

IP 地址:	141.14.2.21
	10001101 00001110 00000010 00010101
子网掩码:	255.255.255.0
	11111111 11111111 11111111 00000000
网络地址:	141.14.2.0
	10001101 00001110 00000010 00000000

(b) 划分子网

图 3.6 进行按位“与”(AND)运算可得到网络地址

图 3.6(a)表示在没划分子网情况下,网络地址是 IP 地址与它默认的子网掩码(255.255.0.0)按位“与”(AND)运算的结果,即将主机号 host-id 置为 0 的 IP 地址。图 3.6(b)表示在划分子网情况下,在主机号借用 8 位作为子网号 subnet-id,子网掩码中的“1”个数相应地增加 8,即(255.255.255.0)。这时将子网掩码和 IP 地址按位“与”(AND)运算就得到了子网地址。这里要注意:网络地址(在划分子网时常称为子网地址)并不仅仅是一个子网号 subnet-id,而是将主机号 host-id 置为 0 的 IP 地址。可以看出,子网掩码不能单独存在,它必须结合 IP 地址一起使用。

与 IP 地址相同,子网掩码也通常使用点分十进制表示法表示,例如 255.255.255.0、255.255.255.240 等。有时为了表示方便,通常在 IP 地址后加一个“/网络号和子网号位数”。例如,210.45.12.58/28 就表示该 IP 地址的网络号 net-id 和子网号 subnet-id 共占用 28 位,主机号占用  $32-28=4$  位,如果用点分十进制表示法表示,则子网掩码是 255.255.255.240(11111111.11111111.11111111.11110000)。

使用子网掩码的好处就是:不管网络有没有划分子网,也不管 IP 地址中的网络号 net-id 和子网号 subnet-id 是多少位,只要将子网掩码和 IP 地址进行按位“与”(AND)运算,就立即得出网络地址来,这样在路由器处理到来的 IP 分组就可采用同样的算法。

如果一个网络不划分子网,那么该网络的子网掩码就使用默认子网掩码。默认子网掩码中值为 1 的位和 IP 地址的网络号 net-id 所占位正好相对应。因此默认子网掩码和不划分子网的 IP 地址按位“与”(AND)运算,就得出该 IP 地址的网络地址来,这样做就可以不用查找该地址的分类位就能知道这是哪一类的 IP 地址。显然,A 类、B 类和 C 类网络默认子



网掩码分别是 255.0.0.0(/8)、255.255.0.0(/16)、255.255.255.0(/24)，如图 3.7 所示。

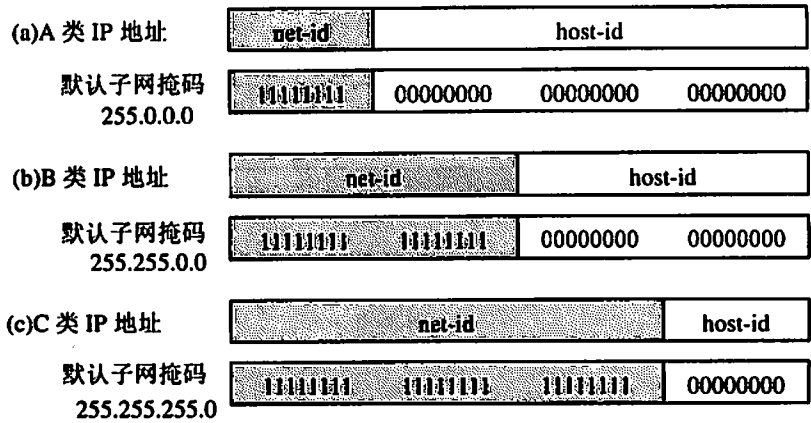


图 3.7 A 类、B 类和 C 类 IP 地址默认子网掩码

4. 划分子网实例

(1) B 类地址的子网规划示例

B 类地址由两个字节的网络号 net-id 和两个字节的主机号 host-id 组成。一个得到 B 类地址的组织可以有一个单独的物理网络，在此网络上连接的计算机可达 65534( $2^{16}-2$ )个。但是，若该组织愿意有更多的物理网络，则这个大的范围可划分成许多更小的范围，表 3.4 说明了一个 B 类地址可以有多少种子网划分的方法。在采用固定长度子网时，划分的所有子网的子网掩码都是相同的。

表 3.4 B 类地址的子网划分选择(使用固定长度子网)

子网位数	子网掩码	子网数	主机数
2	255.255.192.0	2	16382
3	255.255.224.0	6	8190
4	255.255.240.0	14	4094
5	255.255.248.0	30	2046
6	255.255.252.0	62	1022
7	255.255.254.0	126	510
8	255.255.255.0	254	254
9	255.255.255.128	510	126
10	255.255.255.192	1022	62
11	255.255.255.224	2046	30
12	255.255.255.240	4094	14
13	255.255.255.248	8190	6
14	255.255.255.252	16382	2

例如，一个具有 B 类地址组织，网络号为 X.Y.0.0( $128 \leq X \leq 191$ )，需要至少 12 个子网，试找出子网掩码和每个子网的配置。因为需要至少 12 个子网，划分时至少要 14 个子网，12



个是可用的, 两个保留为特殊地址不可用, 因此至少需要向主机号 host-id 借 4 位( $2^3-2 \leq 12 \leq 2^4-2$ )来构造子网, 网络号 net-id 和子网号 subnet-id 共 12 位( $8+4=12$ ), 所以子网掩码为 11111111.11111111.11110000.00000000, 即 255.255.240.0。每个子网有 4096 个( $2^{12}=4096$ )地址, 其中第一个地址用来定义子网(子网地址), 而最后一个地址用于子网内广播(广播地址), 这就表明连接到每一个子网上的计算机数最多是 4094。表 3.5 是每一个子网的地址范围。

表 3.5 B 类地址的子网划分实例(使用固定长度子网)

子网	子网地址	地址范围	广播地址	说明
第 0 个子网	X.Y.0.0	X.Y.0.1~X.Y.15.254	X.Y.15.255	保留, 不可用
第 1 个子网	X.Y.16.0	X.Y.16.1~X.Y.31.254	X.Y.31.255	可用
第 2 个子网	X.Y.32.0	X.Y.32.0~X.Y.47.254	X.Y.47.255	可用
⋮	⋮	⋮	⋮	可用
第 14 个子网	X.Y.224.0	X.Y.224.0~X.Y.239.254	X.Y.239.255	可用
第 15 个子网	X.Y.240.0	X.Y.240.1~X.Y.255.254	X.Y.255.255	保留, 不可用

注意: 根据 RFC950 规定, 进行子网划分时, 对于子网号 subnet-id 为全 0 和全 1 的子网不允许使用, 因此上表中, 第 0 个子网和第 15 个子网是不可用的。但随着无分类域间路由选择 CIDR 的广泛使用, 现在全 0 和全 1 的子网也可以使用, 但一定要谨慎使用, 要弄清所使用的路由器是否支持全 0 和全 1 的子网。

## (2) C 类地址的子网规划示例

C 类地址由三个字节的网络号 net-id 和一个字节的主机号 host-id 组成。一个得到 C 类地址的组织可以有一个单独的物理网络, 在此网络上连接的计算机可达 254( $2^8-2$ )个。但是, 若该组织愿意有更多的物理网络, 则这个大的范围可划分成许多更小的范围, 表 3.6 说明了一个 C 类地址可以有多少种子网划分的方法。(在采用固定长度子网时, 划分的所有子网的子网掩码都是相同的)。

表 3.6 C 类地址的子网划分选择(使用固定长度子网)

子网位数	子网掩码	子网数	主机数
2	255.255.255.192	2	62
3	255.255.255.224	6	30
4	255.255.255.240	14	14
5	255.255.255.248	30	6
6	255.255.255.252	62	2

例如, 一个具有 C 类地址的组织, 网络号为 X.Y.Z.0( $192 \leq X \leq 223$ ), 需要至少 5 个子网, 试找出子网掩码和每个子网的配置。因为需要至少 5 个子网, 划分时至少要 7 个子网, 5 个是可用的, 两个保留为特殊地址不可用, 因此至少需要向主机号 host-id 借 3 位( $2^2-2 \leq 5 \leq 2^3-2$ )来构造子网, 网络号 net-id 和子网号 subnet-id 共 27( $24+3$ )位, 所以子网掩码为 11111111.11111111.11111111.11100000, 即 255.255.255.224。每个子网有 32 个( $2^5=32$ )地址, 其中第一个地址用来定义子网(子网地址), 而最后一个地址用于子网内广播(广播地址), 这

就表明连接到每一个子网上的计算机数最多是 30。表 3.7 是每一个子网的地址范围。

A 类地址的子网规划方法和 B 类、C 类相似, 因篇幅所限, 这里不做详细介绍。

表 3.7 C 类地址的子网划分实例(使用固定长度子网)

子网	子网地址	地址范围	广播地址	说明
第 0 个子网	X.Y.Z.0	X.Y.Z.1~X.Y.Z.30	X.Y.Z.31	保留, 不可用
第 1 个子网	X.Y.Z.32	X.Y.Z.33~X.Y.Z.62	X.Y.Z.63	可用
第 2 个子网	X.Y.Z.64	X.Y.Z.65~X.Y.Z.94	X.Y.Z.95	可用
⋮	⋮	⋮	⋮	可用
第 6 个子网	X.Y.Z.192	X.Y.Z.193~X.Y.Z.222	X.Y.Z.223	可用
第 7 个子网	X.Y.Z.224	X.Y.Z.225~X.Y.Z.254	X.Y.Z.255	保留, 不可用

### 5. 变长子网掩码 VLSM

因特网允许一个地点使用变长子网划分。举个例子看看什么时候有这种需要。考虑有一个具有 C 类地址的地点需要划分为 5 个子网, 其连接的主机数分别为: 60、60、60、30 和 30。这个地点不能使用给子网分配两个位的掩码, 因为这样将只有 4 个可连接 62 台主机( $256/4=62$ )的子网。在这个地点使用给子网分配三个位的掩码也不行, 因为这样将有 8 个可连接 30 台主机( $256/8=30$ )的子网。(应注意, 这里放松了对特殊地址的要求, 即子网号为全 0 和全 1 可用。)

解决这个问题的一种方法是使用变长子网划分。在这种配置中, 路由器使用两个不同的掩码。它先使用具有 26 个 1 的掩码(11111111.11111111.11111111.11000000 或 255.255.255.192), 将网络划分为 4 个子网。然后再对其中的一个子网使用具有 27 个 1 的掩码(11111111.11111111.11111111.11100000 或 255.255.255.224), 将其划分为两个更小的子网(见图 3.8)。

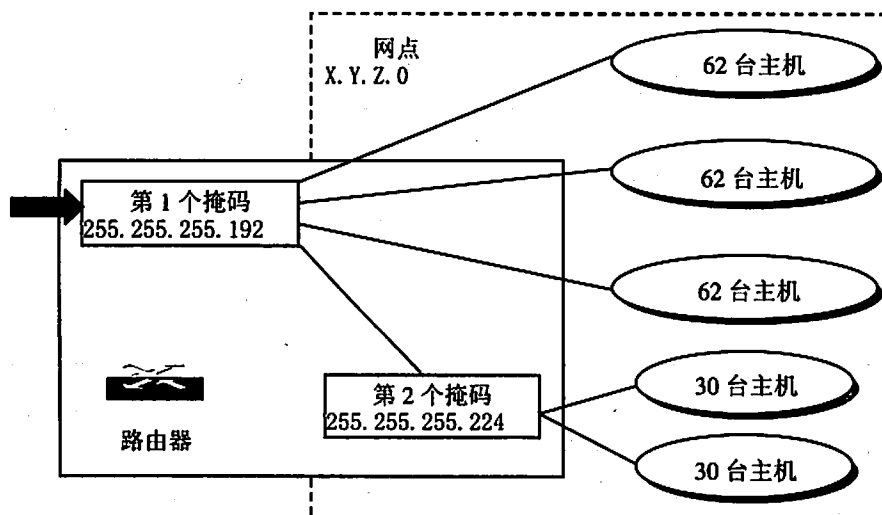


图 3.8 变长子网划分

### 3.1.1.3 超网(Supernet)和无分类编址(CIDR)

虽然 A 类和 B 类地址几乎用完了, 但 C 类地址目前还能申请到。然而 C 类地址空间只能容纳最多 254 台主机, 这可能无法满足一个组织的需要, 甚至一个中等规模的组织也会需要更多的地址。

一种解决问题的方法是构成超网(Supernet)。为此, 一个组织可申请一块而不是只申请一个 C 类地址。例如, 一个需要 1000 个地址的组织可申请 4 个 C 类地址。这个组织就可以在一个超网中、在 4 个网络中或在超过 4 个子网中使用这些地址。在图 3.9 中, 4 个 C 类地址合并为一个超网。

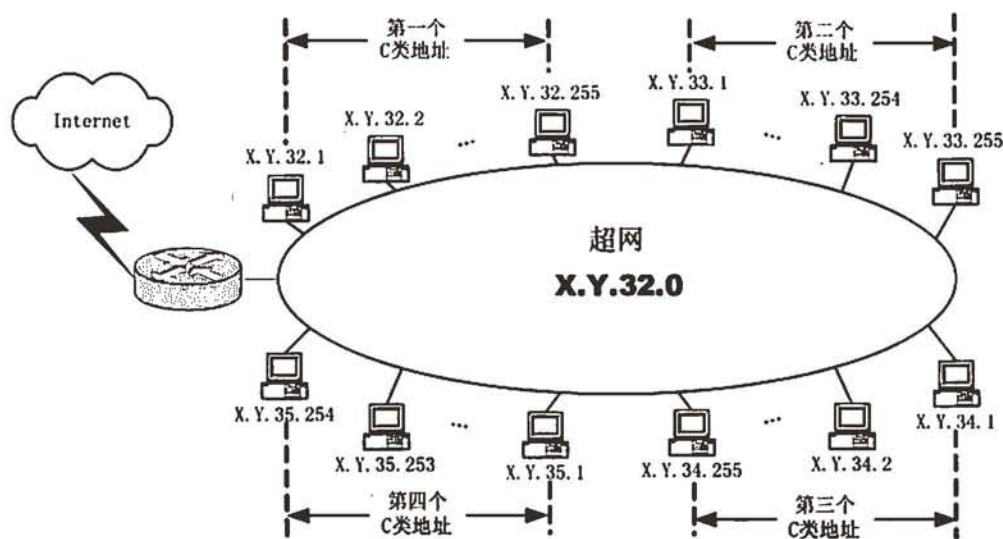


图 3.9 超网

可以给超网掩码指派一块 C 类网络地址, 只要地址数是 2 的整数次方(2, 4, 8, 16, ...) 即可。C 类地址的默认掩码是 255.255.255.0, 即 24 个 1 后面跟上 8 个 0。如果将其中的某些 1 改变为 0, 我们就可得到一组 C 类地址的超网掩码。如图 3.10 所示, 超网掩码与子网掩码中的一些做法相反。在子网掩码中, 我们将默认掩码中的 host-id 部分的某些 0 改变为 1。在超网掩码中, 我们将 net-id 部分中的某些 1 改变为 0。要注意到, 在超网掩码中全 1 的位置定义了最低地址。例如, 如图 3.10 所示的超网掩码, 开始地址可以是 X.Y.32.0, 但不能是 X.Y.33.0。将最低地址与超网掩码组合起来就能惟一地定义属于一个超网的地址范围, 另一个定义地址范围的方法是使用最低地址和在此范围内的地址数来定义。

例如, 用超网掩码 255.255.252.0 可以将 4 个 C 类地址合并成为一个超网。如果我们选择的第一个地址是 X.Y.32.0, 则其他三个地址就是 X.Y.33.0、X.Y.34.0 和 X.Y.35.0。当路由器收到一个分组时, 就将超网掩码与目的地址作按位“与”(and)运算, 并将结果与最低地址相比较。若结果与最低地址一致, 则该分组就属于这个超网。

假定一个分组到达目的地址 X.Y.33.4。在同掩码 255.255.252.0 作按位“与”(and)运算后, 结果为 X、Y、32、0, 它与最低地址一致, 因此该分组属于这个超网。

现在假定目的地址为 X.Y.39.12 的分组到达。在同掩码 255.255.252.0 作按位“与”(and)

运算后, 结果为 X.Y.36.0, 它与最低地址不一致, 因此该分组不属于这个超网。

在 VLSM 的基础上又进一步研究出无分类编址方法, 它的正式名称是无分类域间路由选择(CIDR, Classless Inter-Domain Routing)。CIDR 最主要的特点有两个:

一是 CIDR 消除了传统 A 类、B 类和 C 类地址以及划分子网的概念, 从而更加有效地分配 IPv4 的地址空间。CIDR 使用各种长度的“网络前缀”(network-prefix)来代替分类地址中的网络号和子网号, 而不像分类地址中只使用 1 字节、2 字节和 3 字节长的网络号。CIDR 不再使用“子网”概念而使用网络前缀, 使 IP 地址从三级编址(使用子网掩码)又回到两级编址, 但这是一个无分类的两级编址。CIDR 使用“斜线记法”, 它又称为 CIDR 记法, 即在 IP 地址后面加上一个斜线“/”, 然后写上网络前缀所占的位数(这个数值对应于三级编址中子网掩码中位 1 的个数)。例如, 128.14.146.158/20, 表示在这 32 位中, 前 20 位表示网络前缀, 而后面 12 位为主机号。

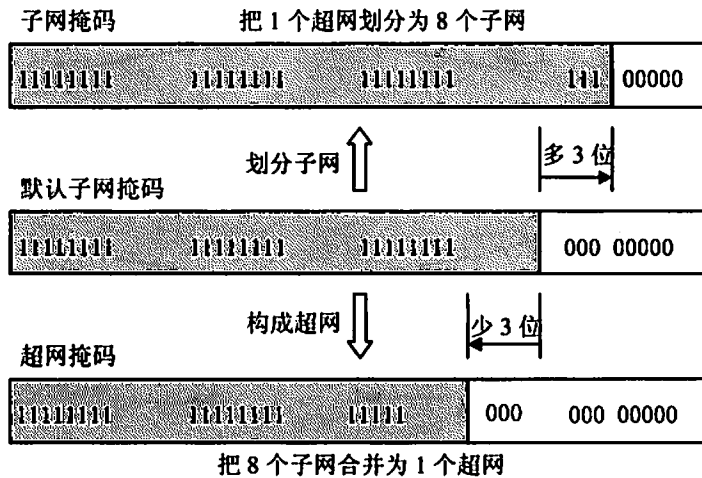


图 3.10 超网掩码

二是 CIDR 将网络前缀都相同的连续的 IP 地址组成“CIDR 地址块”。一个 CIDR 地址块是由地址块的起始地址(即地址块中地址数值最小的一个)和地址块中的地址数来定义的。CIDR 地址块也可用斜线记法来表示, 例如, 128.14.32.0/20 表示的地址块共有  $2^{12}$  个地址, 而这个地址的起始地址是 128.14.32.0。

### 3.1.2 典型例题分析

例 1 一个园区网内某 VLAN 中的网关地址设置为 195.26.16.1, 子网掩码设置为 255.255.240.0, 则 IP 地址 (1) 不属于该 VLAN。该 VLAN 最多可以配置 (2) 台主机。(2004 年下半年网络管理员上午试题 42-43)

- (1) A. 195.26.15.3                      B. 195.26.18.128  
       C. 195.26.24.254                  D. 195.26.31.64
- (2) A. 1021                      B. 1024                      C. 4093                      D. 4096

分析: 该题主要考查考生对 IP 地址规划和超网的掌握情况。



题中提到的 IP 地址是一个 C 类地址, 一个 C 类地址最多可有 254 台主机。当一个大的网络需要更多的主机时, 通常把一个连续的 C 类地址块组成一个超网, 从而提供了更大的地址空间, 超网的地址空间大小是由超网掩码来确定的。超网掩码的运算过程和子网掩码基本一致, 多数时候把这两个概念混同。

一般来说, 在一个 VLAN 中, 所有主机(包括网关)必须有相同的网络地址(超网地址), 由于网关地址为 195.26.16.1, 子网掩码(超网掩码)为 255.255.240.0, 则网络地址(超网地址)是 195.26.16.0, 广播地址为 195.26.31.255, 地址范围为 195.26.16.1~195.26.31.254, 运算过程如图 3.11 所示。

195.26.16.1:	11000011 . 00011010 . 0001	0000 . 00000001
255.255.240.0:	11111111 . 11111111 . 1111	0000 . 00000000
超网地址:	11000011 . 00011010 . 0001	0000 . 00000000
	195 . 26 . 16	. 0
广播地址:	11000011 . 00011010 . 0001	1111 . 11111111
	195 . 26 . 31	. 255

图 3.11 例 1 的运算过程

在(1)的选项中, B、C、D 都属于上述的地址范围, 而选项 A 不在此范围内。

由于子网掩码(超网掩码)是 255.255.240.0, 也就是说网络号(超网号)共占用 20 位, 则主机号占用 12 位, 共有  $2^{12}=4096$  种组合, 但需要除去一个用于标识网络的网络地址和一个用于网内广播的广播地址, 同时该 VLAN 的网关占用一个 IP 地址, 因此实际可分配到主机的地址只有  $4096-2-1=4093$  个。因此(2)的答案是 C。

答案: (1) A (2) C

**例 2** 局域网的 IP 地址范围限定在 192.168.10.17~192.168.10.30 之间, 子网掩码应设置为多少? (2004 年下半年网络管理员下午试题三的【问题 5】, 略有改动)

分析: 该题主要考查考生对子网掩码的理解。

该题可有两种解法:

方法一: IP 地址从 192.168.10.17 到 192.168.10.30 共有 14 个, 再加子网地址 192.168.10.16, 直接广播地址 192.168.10.31, 共有 16 个。这是 C 类地址, 默认使用 8 位作主机号, 需借 4 位作为子网号 ( $2^4=16$ ), 因此子网掩码为 11111111.11111111.11111111.11110000, 转换为十进制为 255.255.255.240。

方法二: 将这 16 个 IP 地址全部转换为二进制, 然后找到它们相同的位数, 使得主机号包含不同位的所有组合, 如图 3.12 所示。

这 16 个 IP 地址有 28 位是相同的, 后 4 位包含了所有组合, 即从 0000 到 1111, 故子网掩码为 11111111.11111111.11111111.11110000, 转换为十进制为 255.255.255.240。

答案: 255.255.255.240

**例 3** 阅读以下说明, 回答问题 1~5, 将解答填入对应的答案栏内。

192.168.10.16:	11000000	10101000	00001010	0001	0000
192.168.10.17:	11000000	10101000	00001010	0001	0001
...	...	...	...	...	...
192.168.10.30:	11000000	10101000	00001010	0001	1110
192.168.10.31:	11000000	10101000	00001010	0001	1111
	← 28 位相同, 作为子网地址 →				← 主机 →

图 3.12 例 2 的运算过程

【说明】

某单位有一个网络, 其中有一台主机的 IP 地址是 193.1.1.165。请回答以下问题:

【问题 1】这个地址是一个什么类型的地址?

【问题 2】它的默认子网掩码是什么?

【问题 3】若子网掩码是 255.255.255.224, 则这台主机所在的子网地址是什么?

【问题 4】该子网的广播地址是什么?

【问题 5】这个 IP 地址所在的子网的主机 ID 范围是什么?

分析: 该题主要考查考生对 IP 地址的分类和子网掩码的掌握情况。

问题 1: 193.1.1.165 用二进制表示为 11000001.00000001.00000001.10100101, 它的前三位为 110, 因此这个 IP 地址是一个 C 类 IP 地址。

问题 2: 由于该 IP 地址是一个 C 类 IP 地址, 则默认子网掩码是 255.255.255.0。

问题 3: 子网掩码为 255.255.255.224, 二进制表示为 11111111.11111111.11111111.11100000, 使用 3 位作为子网号, 5 位作为主机号。这台主机所在的子网地址可以通过将该 IP 地址和子网掩码进行按位“与”(AND)运算求得:

将 11000001.00000001.00000001.10100000 转换为十进制为 193.1.1.160, 该地址就是这台主机所在的子网地址。

问题 4: 广播地址是主机号各位全为“1”的 IP 地址, 它用于全网广播。在该题中, 将主机号全部置为 1, 得到 11000001.00000001.00000001.10111111, 把它转换为十进制为 193.1.1.191, 这个地址就是该子网的广播地址。

问题 5: 子网的主机号范围就是网络地址和广播地址之间的地址(两者都不包括), 于是可以得到 193.1.1.161~193.1.1.190, 可以有 30 台主机。计算过程如图 3.13 所示。

	网络				子网	主机
193.1.1.165:	11000001	00000001	00000001	101	00101	
255.255.255.224:	11111111	11111111	11111111	111	00000	
子网地址:	11000001	00000001	00000001	101	00000	
	193	1	1			160
广播地址:	11000001	00000001	00000001	101	11111	
	193	1	1			191

图 3.13 例 3 的运算过程

答案:

【问题 1】C 类 IP 地址

【问题 2】255.255.255.0

【问题 3】193.1.1.160

【问题 4】193.1.1.191

【问题 5】193.1.1.161~193.1.1.190

例 4 阅读以下说明, 回答问题 1~5, 将解答填入对应的答案栏内。

【说明】

某公司申请了一个 C 类地址 200.200.200.0, 公司的生产部门和市场部门需要划分为单独的网络, 即需要划分 2 个子网, 每个子网至少支持 40 台主机(使用固定子网掩码)。

【问题 1】确定子网掩码。

【问题 2】计算新的子网网络 ID。

【问题 3】每个子网有多少主机地址?

【问题 4】200.200.200.88 所在子网的网络地址是什么?

【问题 5】200.200.200.88 所在子网的广播地址是什么?

分析: 该题主要考查考生对子网划分的掌握情况。

问题 1: 划分子网的第一步是确定子网掩码。对于一个 C 类地址来说, 其默认子网掩码是 255.255.255.0, 也就是有 8 位是用作主机号, 要进行子网划分, 就要从主机号借用若干位作为子网地址, 那么借多少位呢? 题中要求划分为两个子网, 每个子网至少有 40 台主机, 则

$$2^n - 2 \geq 2(\text{子网数})$$

$$2^{8-n} - 2 \geq 40(\text{主机数})$$

解这个不等式, 得  $n=2$ , 即需从主机号借用 2 位用作子网号 subnet-id。C 类地址的默认网络位数是 24 位, 再增加两位, 共 26 位, 即 11111111.11111111.11111111.11000000, 转换为十进制为 255.255.255.192。子网划分见表 3.8。

问题 2: 由于有 2 位用作子网号 subnet-id, 因此共有四种组合 00、01、10、11, 其中 00 和 11 这两种组合的子网号 subnet-id 为全 0 和全 1, 根据 RFC950 规定, 这两个子网是不允许使用的, 因此最后 8 位只能为 01000000 和 10000000, 即 64 和 128, 于是新的子网网络 ID 分别为 200.200.200.64 和 200.200.200.128。

表 3.8 例 4 子网划分(使用固定长度子网)

子网	子网地址	地址范围	广播地址	说明
0	200.200.200.0	200.200.200.1 ~ 200.200.200.62	200.200.200.63	保留, 不可用
1	200.200.200.64	200.200.200.65 ~ 200.200.200.126	200.200.200.127	可用
2	200.200.200.128	200.200.200.129 ~ 200.200.200.190	200.200.200.191	可用
3	200.200.200.192	200.200.200.193 ~ 200.200.200.254	200.200.200.255	保留, 不可用

问题 3: 由于用 2 位用作子网号 subnet-id, 用作主机号 host-id 只有 6 位, 共有  $2^6=64$

种组合,但要除去第一个组合和最后一个组合,它们分别用作网络地址和广播地址。因此每个子网可有  $2^6-2=62$  台主机。

问题 4 和问题 5 的分析同例 1,这里就不再分析了。200.200.200.88 所在子网的网络地址是 200.200.200.64,所在子网的广播地址是 200.200.200.127。计算过程如图 3.14 所示。

	网络			子网	主机
200.200.200.88:	11001000 .	11001000 .	11001000 .	01	011000
255.255.255.192:	11111111 .	11111111 .	11111111 .	11	000000
子网地址:	11001000 .	11001000 .	11001000 .	01	000000
	200 .	200 .	200 .		64
广播地址:	11001000 .	11001000 .	11001000 .	01	111111
	200 .	200 .	200 .		127

图 3.14 例 4 的运算过程

答案:

【问题 1】255.255.255.192

【问题 2】200.200.200.64、200.200.200.128

【问题 3】62

【问题 4】200.200.200.64

【问题 5】200.200.200.127

例 5 阅读以下说明,回答问题 1~3,将解答填入对应的答案栏内。

【说明】

随着网络应用的日益广泛,接入网络和边缘网络的需求也更加复杂多样,企业为了开展电子商务,必须实现与 Internet 的互联,路由器是实现这一互联的关键设备,路由器可以为企业提供更多的智能化服务,包括安全性、可用性和服务质量(QoS)等。下面是 Cisco VLSM 子网设计与路由器的路由选择协议(其中路由器的路由选择协议未列出)。

下面以某公司 VLSM(Variable Length Subnet Mask,变长子网掩码)子网的设计方法为例进行说明。假设该公司被分配了一个 C 类地址,该公司的网络拓扑结构如图 3.15 所示。其中有 4 个部门,每个部门最多有 26 台主机;有 3 个部门,每个部门最多有 10 台主机,它们之间用 4 个点到点串行链路相连。假如分配的网络为 202.128.236.0。请注意:

(1) 该单位的路由器不支持全 0 和全 1 子网。

(2) 为保证答案的惟一,使用较小的地址用于点到点串行链路,较大的地址用于有 10 台主机的子网,最大地址用于有 26 台主机的子网。

【问题 1】请为该网络进行子网分割,至少有 3 个不同变长的子网掩码,请列出你所求的变长子网掩码,并说明理由。

【问题 2】请列出每个单位的网络地址、广播地址和最多可容纳的主机数。

【问题 3】请列出每个串行链路两端的地址。

分析:该题主要考查考生对 VLSM 的理解和操作。

问题 1:首先从具有最大个数主机的网络开始,主机数要至少为 26 台,则主机号必须



要有5位( $2^5-2=30$ )才能满足,所以可划出3位作为子网号,网络号和子网号共27位,这样子网掩码为11111111.11111111.11111111.11100000,即255.255.255.224。把这个网络划分为8个子网,其中子网号全0和全1为不能使用的保留地址,每个子网有32个地址,除去第一个地址用来定义子网(子网地址),最后一个地址用于子网内广播(广播地址),这就表明连接到每一个子网上的计算机数最多是30。各子网的主机号范围如表3.9所示。

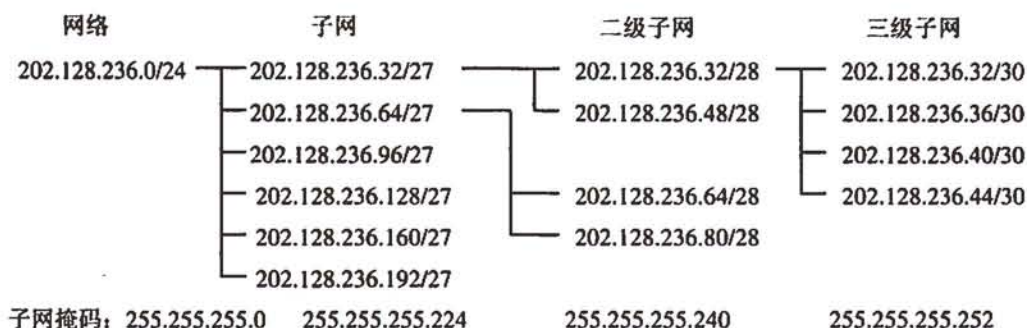


图 3.15 例 5 的子网化过程

表 3.9 202.128.236.0/27 子网化

子网	子网地址	网络号	子网号	主机号	主机号范围 (含网络地址和广播地址)
0	202.128.236.0	11001010.10000000.11101100.	000	00000	保留(0~31)
1	202.128.236.32	11001010.10000000.11101100.	001	00000	子网 1(32~63)
2	202.128.236.64	11001010.10000000.11101100.	010	00000	子网 2(64~95)
3	202.128.236.96	11001010.10000000.11101100.	011	00000	子网 3(96~127)
4	202.128.236.128	11001010.10000000.11101100.	100	00000	子网 4(128~159)
5	202.128.236.160	11001010.10000000.11101100.	101	00000	子网 5(160~191)
6	202.128.236.192	11001010.10000000.11101100.	110	00000	子网 6(192~223)
7	202.128.236.224	11001010.10000000.11101100.	111	00000	保留(224~255)

子网掩码: 使用 27 位, 即 11111111.11111111.11111111.11100000(255.255.255.224)

接下来,为满足每个子网有10台主机的要求,必须对子网进一步子网化。使用子网掩码/28(11111111.11111111.11111111.11110000,即255.255.255.240),对上述两个子网(根据【说明】要求,这里取子网1和子网2)进一步子网化,划分成4个二级子网(子网1-1、子网1-2和子网2-1、子网2-2),每个子网共有14台主机( $2^4-2=14$ )。

最后,为点到点的广域网链路分配IP地址。由于点到点的串行链路需要的地址少,只要2个地址用在每一条链路的两端上的每一个路由器上。从4个二级子网中取一个(根据【说明】要求,这里取第一个二级子网1-1),使用30位子网掩码(11111111.11111111.11111111.11111100,即255.255.255.252)再进一步子网化,得到了4个三级子网(子网1-1-1、子网1-1-2、子网1-1-3和子网1-1-4),每个子网中可用的主机地址有两个(实际上每个子网中有4个主机地址,它包括子网号、广播地址以及2个可分配的地址)。

划分过程可用图 3.15 来表示。

综上所述, 三个变长子网掩码分别是 255.255.255.224、255.255.255.240 和 255.255.255.252。

· 问题 2: 根据问题 1 的分析, 取表 3.9 中子网 3、4、5、6 用作有 26 台主机的子网; 子网 1-2 和子网 2-1、子网 2-2 用作有 10 台主机的子网, 其网络地址、子网掩码、广播地址和主机号范围如表 3.10 所示。

表 3.10 202.128.236.0/27 子网化

子网	子网地址	子网掩码	主机范围	广播地址
子网 1-2	202.128.236.48	255.255.255.240	202.128.236.(49~62)	202.128.236.63
子网 2-1	202.128.236.64	255.255.255.240	202.128.236.(65~78)	202.128.236.79
子网 2-2	202.128.236.80	255.255.255.240	202.128.236.(81~94)	202.128.236.95
子网 3	202.128.236.96	255.255.255.224	202.128.236.(97~126)	202.128.236.127
子网 4	202.128.236.128	255.255.255.224	202.128.236.(129~158)	202.128.236.159
子网 5	202.128.236.160	255.255.255.224	202.128.236.(161~190)	202.128.236.191
子网 6	202.128.236.192	255.255.255.224	202.128.236.(193~222)	202.128.236.223

问题 3: 根据问题 1 的分析和图 3.15 可知, 四个点到点的串行链路的网络地址分别是: 202.128.236.32/30、202.128.236.36/30、202.128.236.40/30 和 202.128.236.44/30, 因此, 这四条点到点的串行链路的地址分别为。

第一条: 202.128.236.33 和 202.128.236.34;

第二条: 202.128.236.37 和 202.128.236.38;

第三条: 202.128.236.41 和 202.128.236.42;

第四条: 202.128.236.45 和 202.128.236.46。

答案: 略

### 3.1.3 同步练习

1. 阅读以下说明, 回答问题 1~5, 将解答填入对应的答案栏内。

【说明】

某单位有一个网络, 其中有一台主机的 IP 地址是 156.108.204.29。请回答以下问题:

【问题 1】这个地址是一个什么类型的地址? 不划分子网时, 其网络地址是什么? 广播地址是什么?

【问题 2】它的默认子网掩码是什么?

【问题 3】若子网掩码是 255.255.255.248, 则这台主机所在的子网地址是什么?

【问题 4】该子网的广播地址是什么?

【问题 5】这个 IP 地址所在子网的主机 IP 范围是什么?

2. 阅读以下说明, 回答问题 1~问题 4, 将解答填入对应的答案栏内。

【说明】

某公司申请了一个 C 类地址 210.45.12.0，公司共有 12 个子网，每个子网至少支持 12 台主机(使用固定子网掩码)。

【问题 1】确定子网掩码。

【问题 2】每个子网有多少主机地址？

【问题 3】210.45.12.100 所在子网的网络地址是什么？

【问题 4】210.45.12.100 所在子网的广播地址是什么？

3. 阅读以下说明，回答问题 1~3，将解答填入对应的答案栏内。

【说明】

随着网络应用的日益广泛，接入网络和边缘网络的需求也更加复杂多样，企业为了开展电子商务，必须实现与 Internet 的互连，路由器是实现这一互连的关键设备，路由器可以为企业提供更多的智能化服务，包括安全性、可用性和服务质量(QoS)等。

下面是某公司，VLSM(Variable Length Subnet Mask，变长子网掩码)子网的设计方法。假设该公司被分配了一个 C 类地址，该公司的网络拓扑结构如图 3.16 所示。其中部门 A 拥有主机数 20、部门 B 拥有主机数 10、部门 C 拥有主机数 20、部门 D 拥有主机数 10。分公司 A 拥有主机数 10、分公司 C 拥有主机数 10。假设分配的网络为 192.168.1.0。

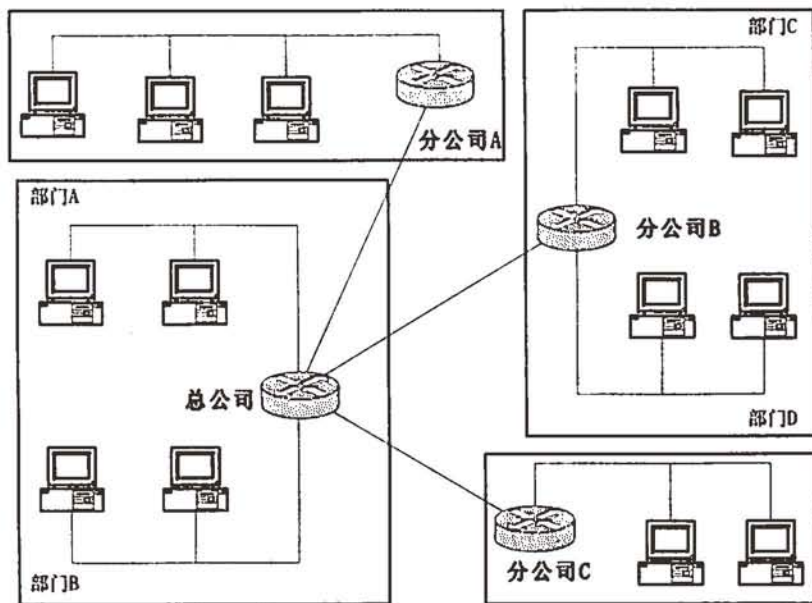


图 3.16 同步练习 3 示意图

【问题 1】请为该网络进行子网分割，至少有 3 个不同变长的子网掩码，请列出您所求的变长子网掩码，并说明理由。注意：该单位的路由器不支持全 0 和全 1 子网。

【问题 2】请列出您所分配的网络地址。

【问题 3】为该网络分配广域网地址。

### 3.1.4 同步练习参考答案

1.

【问题 1】这是一个 B 类 IP 地址，不划分子网时，其网络地址是 156.108.0.0，广播地址是 156.108.255.255。

【问题 2】默认子网掩码 255.255.0.0。

【问题 3】这台主机所在的子网地址是 156.108.204.24。

【问题 4】该子网的广播地址是 156.108.204.31。

【问题 5】这个 IP 地址所在的子网的主机 IP 范围是 156.108.204.25~156.108.204.30。

2.

【问题 1】255.255.240.0

【问题 2】14

【问题 3】210.45.12.96

【问题 4】210.45.12.111

3.

【问题 1】255.255.255.224、255.255.255.240、255.255.255.252。原因同例 5 分析，划分过程如图 3.17 所示。(注：划分的方法很多，下面只是其中的一种。)

【问题 2】将 192.168.1.48/28 分配给部门 B、192.168.1.64/28 分配给部门 D、192.168.1.80/28 分配给分公司 A、192.168.1.96/28 分配给分公司 C、192.168.1.112/28 保留为网络扩展、192.168.1.128/27 分配给部门 A、192.168.1.160/27 分配给部门 C、192.168.1.192/27 保留为网络扩展。



图 3.17 同步练习 3 的答案

【问题 3】把 192.168.1.33 和 192.168.1.34 分配给部门 A 和分公司 A 之间的串行线路；  
把 192.168.1.37 和 192.168.1.38 分配给部门 A 和部门 C 之间的串行线路；  
把 192.168.1.33 和 192.168.1.34 分配给部门 A 和分公司 C 之间的串行线路；  
192.168.1.44/30 子网中 192.168.1.45 和 192.168.1.46 保留为网络扩展；



## 3.2 DNS 服务器配置

### 3.2.1 考点辅导

#### 3.2.1.1 Windows Server 2003 下 DNS 服务器的安装与配置

##### 1. 安装 DNS 服务

在 Windows Server 2003 默认安装时, DNS 服务并没有安装。这里要注意作为 DNS 服务器的计算机必须有静态 IP 地址和子网掩码, 并设置自己的 IP 地址为首选 DNS 服务器。例如, 服务器的 IP 地址和子网掩码为“192.168.10.10”和“255.255.255.0”, 则本机的 DNS 服务器地址中首选 DNS 服务器地址必须设为“192.168.10.10”或“127.0.0.1”。

在 Windows Server 2003 计算机上安装 DNS 服务器的步骤如下:

(1) 在要安装 DNS 服务的 Windows Server 2003 计算机上单击【开始】|【设置】|【控制面板】, 在控制面板中, 双击【添加/删除程序】, 选择【添加/删除 Windows 组件】, 在【组件】列表框中选取【网络服务】, 如图 3.18 所示。

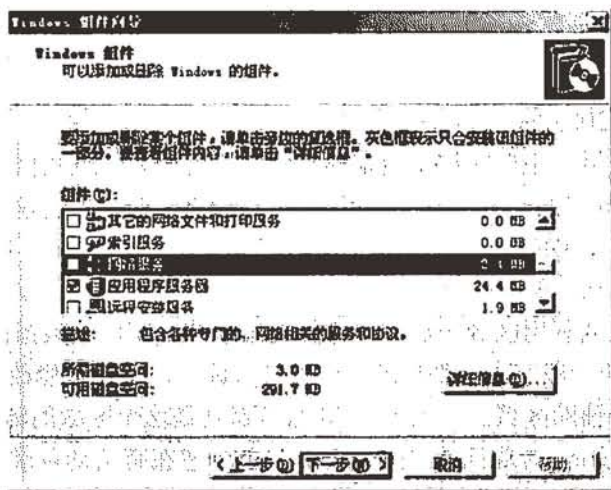


图 3.18 【Windows 组件向导】对话框

(2) 单击【详细信息】按钮, 进入【网络服务】对话框, 选中【域名系统(DNS)】, 如图 3.19 所示。

(3) 单击【确定】按钮, 回到前一个对话框, 再单击【下一步】按钮开始安装 DNS 服务器。

##### 2. 配置计算机成为 DNS 服务器的客户端

(1) 在客户端计算机上打开【TCP/IP 属性】对话框, 选择【使用下面的 DNS 服务器地址】, 在【首选 DNS 服务器】文本框中输入 DNS 服务器 IP 地址, 如“192.168.10.10”。如果网络中还有其他的 DNS 服务器可供选择的话, 在【备用 DNS 服务器】文本框中输入

其他 DNS 服务器 IP 地址，如图 3.20 所示。

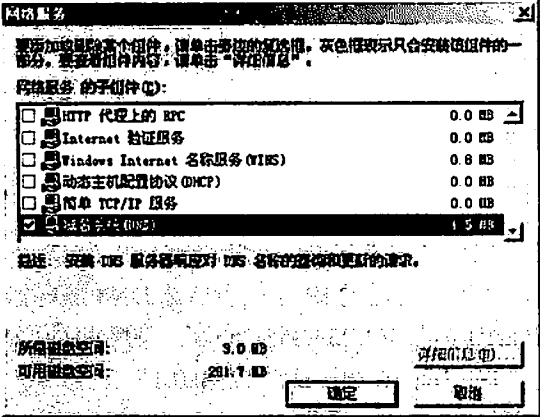


图 3.19 【网络服务】对话框

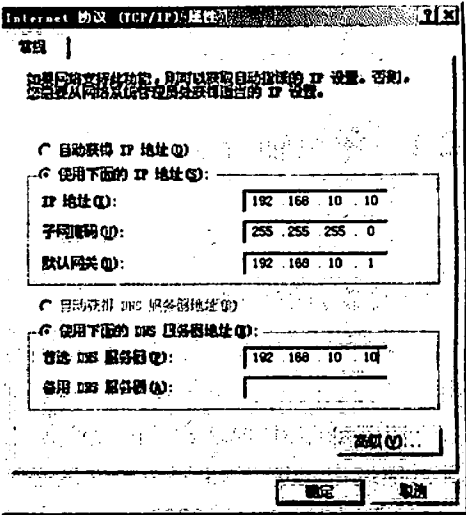


图 3.20 设置 DNS 服务器的 TCP/IP 属性

(2) 单击【确定】按钮，即完成对于 DNS 客户端的设置。

3. 创建 DNS 正向解析区域

必须在 DNS 服务器内创建区域与区域文件，以便位于该区域内的主机数据存储到区域文件内。

Windows Server 2003 的 DNS 服务器支持下述三种区域类型：

- 标准主要区域：主要区域是用来存储此区域内所有主机数据的正本。其区域文件采用 DNS 规格的一般文本文件标准。当在 DNS 服务器创建一个主要区域与区域文件后，这个 DNS 服务器就成为主域名服务器。
- 标准辅助区域：辅助区域是用来存储此区域内所有主机数据的副本，这份数据是从其主要区域利用区域传送的方式复制过来的。存储此数据的区域文件也是采用 DNS 规格的一般文本文件标准，但它是只读的，不能被修改。当在 DNS 服务器内创建一个辅助区域后，这个 DNS 服务器就是这个区域的辅助名称服务器。
- Active Directory(活动目录)集成区域：只能创建在有活动目录的网络环境中，将此区域的主机数据存储存储在域控制器的活动目录内，这份数据会自动被复制到其他域控制器内。

Windows Server 2003 的 DNS 服务器有两种查找区域：

- 正向查找区域：正向查找区域可以让 DNS 客户端利用主机的域名查询其 IP 地址。
- 反向查找区域：反向查找区域可以让 DNS 客户端利用 IP 地址查询主机的域名。

创建 DNS 正向解析区域的步骤如下：

(1) 在 DNS 服务器上，依次选择【开始】|【程序】|【管理工具】|DNS，即打开 DNS 控制台，如图 3.21 所示。

(2) 右击【正向查找区域】，选择【创建新区域】命令，打开【新建区域向导】对话框，如图 3.22 所示。

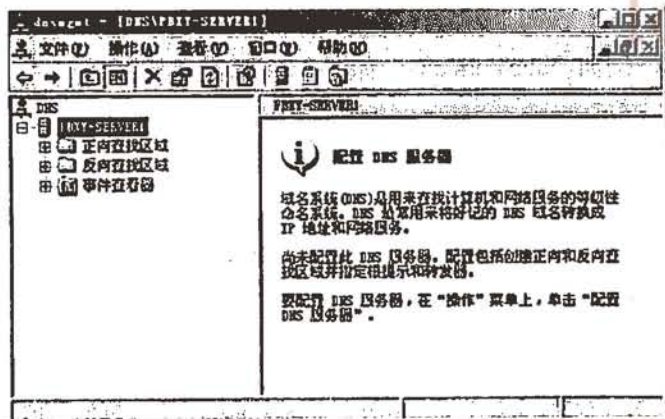


图 3.21 DNS 控制台

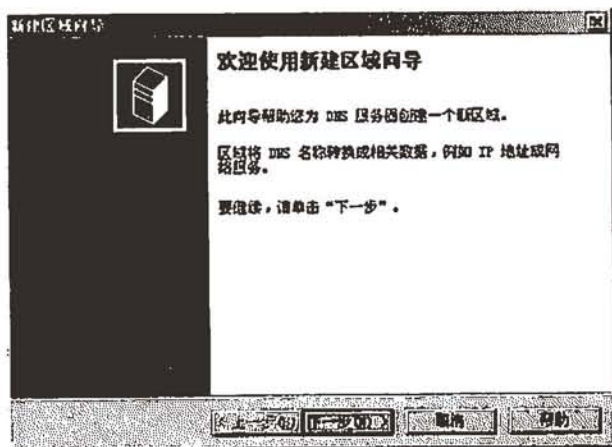


图 3.22 【新建区域向导】对话框

(3) 单击【下一步】按钮，在【区域类型】界面中，选中【主要区域】单选项，如图 3.23 所示。

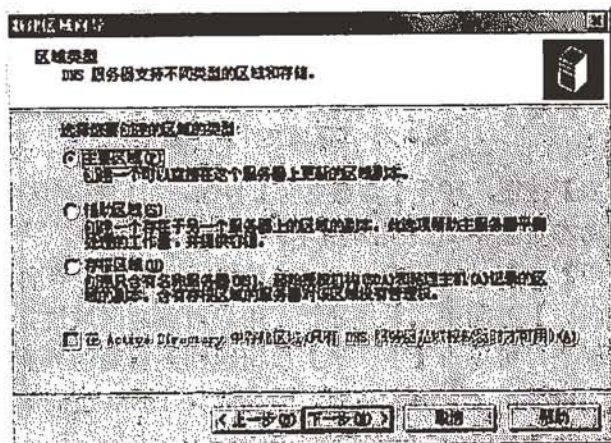


图 3.23 【区域类型】界面

(4) 单击【下一步】按钮, 打开【区域名称】界面, 在“区域名称”文本框中, 为此区域设置区域名称, 例如“abc.com.cn”, 如图 3.24 所示。

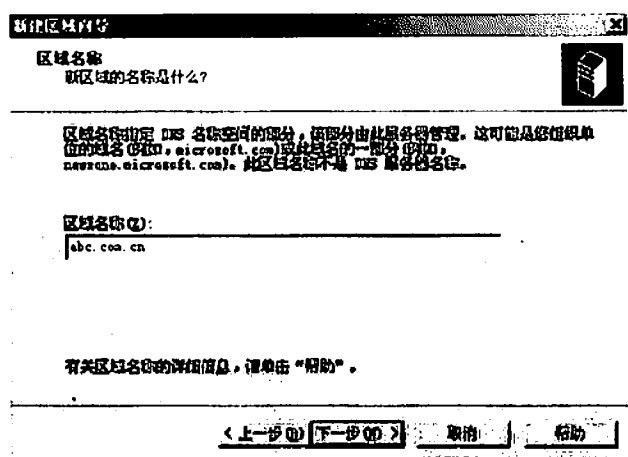


图 3.24 【区域名称】界面

(5) 单击【下一步】按钮, 打开【区域文件】界面, 在【区域文件】界面中, 可以设置区域文件名(新建文件时), 系统会自动在区域名称后加“.dns”作为文件名, 也可以使用一个已有文件, 如图 3.25 所示。

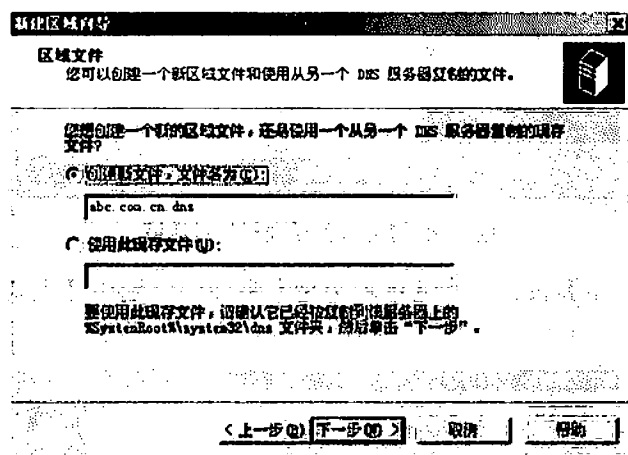


图 3.25 【区域文件】界面

(6) 单击【下一步】按钮, 打开【动态更新】界面, 用户指定这个 DNS 区域是否允许接受安全或不安全的动态更新, 如图 3.26 所示。

(7) 单击【下一步】按钮, 打开【正在完成新建区域向导】界面, 如图 3.27 所示。在【正在完成新建区域向导】界面中, 系统显示了用户对新建区域进行配置的信息, 如果用户认为某项配置需要调整, 可单击【上一步】按钮返回到前面的界面中重新配置。如果确认自己配置正确的话, 可单击【完成】按钮, 即完成对 DNS 正向解析区域的创建, 返回 DNS 控制台以查看区域的状态。



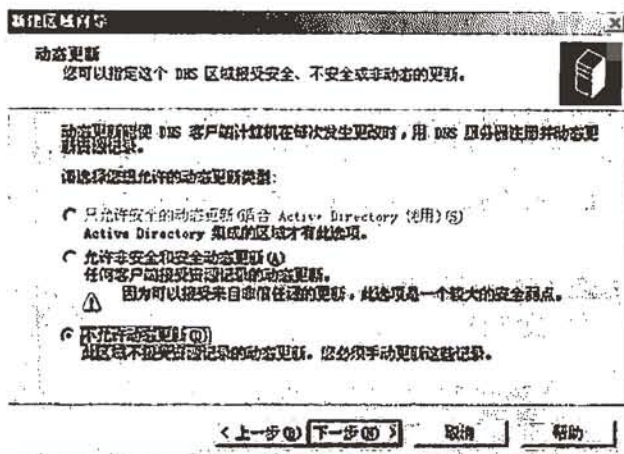


图 3.26 【动态更新】界面

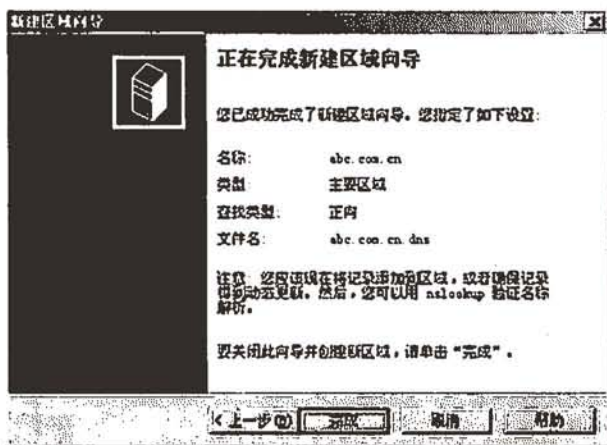


图 3.27 【正在完成新建区域向导】界面

#### 4. 创建 DNS 反向解析区域

反向查找区域可以让 DNS 客户端利用 IP 地址查询其主机的域名，反向查找区域并不是非常必要，但在某些情况下会用得到。

反向区域中，区域名前半段是其网络 ID 的反向书写，而区域名后半段必须是“in-addr.arpa”。例如，如果要针对网络 ID 为“192.168.10.0”的 IP 地址来提供反向解析功能，则此反向区域的名称必须是“10.168.192.in-addr.arpa”。

创建 DNS 反向解析区域的步骤如下：

(1) 在 DNS 服务器上，依次选择【开始】|【程序】|【管理工具】|【DNS】，即打开 DNS 控制台，如图 3.21 所示。

(2) 右击【反向查找区域】，选择【创建新区域】命令，打开【创建新区域向导】对话框，如图 3.22 所示。

(3) 单击【下一步】按钮，打开【区域类型】界面。在【区域类型】界面中，选择【主要区域】单选项，如图 3.23 所示。

(4) 单击【下一步】按钮,打开【反向查找区域名称】界面。在【网络 ID】文本框中输入此区域所支持的反向查询的网络 ID,它会自动在【反向查找区域名称】文本框中设置区域名称。也可以直接在【反向查找区域名称】文本框中设置其区域名称。例如该 DNS 服务器负责“192.168.10.0”这一网络的反向域名解析,可在“网络 ID”文本框中输入“192.168.10”,则在【反向查找区域名称】文本框中显示“10.168.192.in-addr.arpa”,如图 3.28 所示。

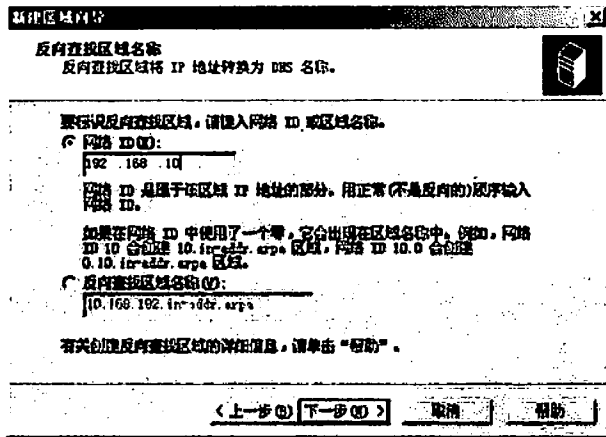


图 3.28 【反向查找区域名称】界面

(5) 单击【下一步】按钮,打开【区域文件】界面。在【区域文件】界面中,输入区域文件名,系统会自动在区域名称后加“.dns”作为文件名并新建一个文件,也可使用一个已有文件,如图 3.29 所示。

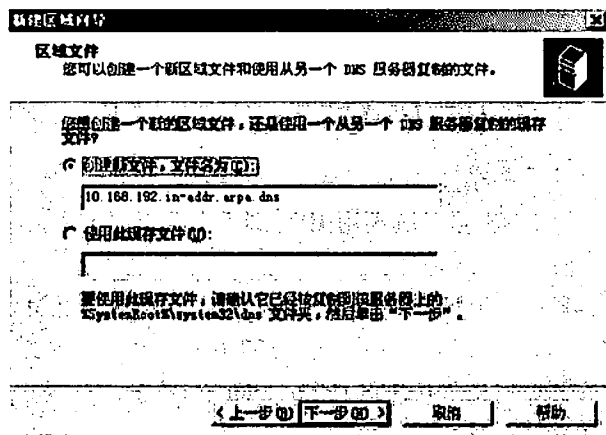


图 3.29 【区域文件】界面

(6) 单击【下一步】按钮,打开【正在完成新建区域向导】界面,如图 3.27 所示。在【正在完成新建区域向导】界面中,系统显示了用户对新建区域进行配置的信息,如果用户认为某项配置需要调整,可单击【上一步】按钮返回到前面的界面中重新配置。如果确认自己配置正确的话,可单击【完成】按钮,即完成对 DNS 反向解析区域的创建,返回 DNS 控制台以查看区域的状态。

### 5. 新建记录到主要区域内

在区域内可以新建主机的相关数据,这些数据被称为“资源记录”,DNS 服务器支持相当多的资源记录,将数据新建到区域内,其步骤如下:

(1) 在 DNS 服务器上,依次选择【开始】|【程序】|【管理工具】|【DNS】,即打开 DNS 控制台。

(2) 选择【正向查找区域】中的“abc.com.cn”区域后右击,弹出快捷菜单。根据要新建的记录,在该弹出的快捷菜单中选择相应的命令。

- **【新建主机】**:将主机的相关数据新建到 DNS 服务器内的区域后,就可以由该 DNS 服务器来实现域名与 IP 地址的映射。选择【新建主机】命令后,打开【新建主机】对话框,如图 3.30 所示。在【新建主机】对话框中输入主机的主机名与 IP 地址,然后单击【添加主机】按钮。
- **【新建别名】**:在某些情况下,需要为区域内的一台主机创建多个主机名称,例如一台主机是 Web 服务器同时又是 FTP 服务器,则可以为该主机取两个不同名称。选择【新建别名】命令后,打开【新建资源记录】对话框,如图 3.31 所示。在【新建资源记录】对话框的【别名】选项卡中输入主机的别名与目标主机的完全合格的域名,然后单击【确定】按钮。

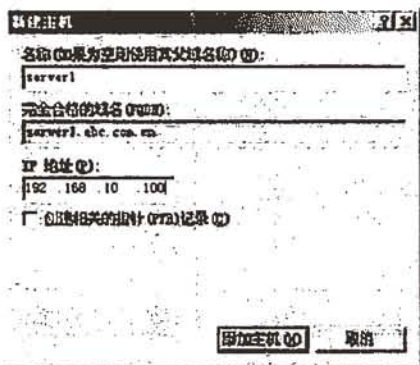


图 3.30 【新建主机】对话框

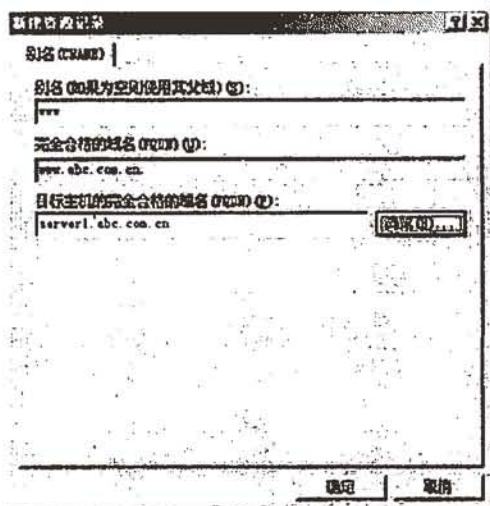


图 3.31 【别名】选项卡

- **【新建邮件交换器】**:当用户将邮件送到本地邮件服务器后,本地邮件服务器必须将邮件送到目的地邮件服务器,而目的地的邮件服务器 IP 地址可以向 DNS 服务器查询。邮件交换器记录就是指定哪些主机负责接收该区域的电子邮件,如果在此区域内创建了多个邮件交换器记录,可以设置邮件服务器的优先级,数字较小的优先级较高。选择【新建邮件交换器】命令后,打开【新建资源记录】对话框,如图 3.32 所示。在【新建资源记录】对话框的【邮件交换器】选项卡中分别输入【主机或子域】、【邮件服务器】的完全合格的域名及【邮件服务器优先级】,然后单击【确定】按钮。

(3) 选择【反向查找区域】中的“10.168.192.in-addr.arpa”区域后右击,在弹出的快捷菜单中选择【新建指针】菜单项,打开【新建资源记录】对话框,如图 3.33 所示。在【新建资源记录】对话框的【新建指针】选项卡中的【主机 IP 号】文本框中,键入主机 IP 地址的最后一个十进制数,在【主机名】文本框中,键入 DNS 主机的完全合格域名,该计算机使用此指针记录提供反向查找(把 IP 地址解析为域名)。单击【确定】按钮,建立新增的指针,新增的指针记录将显示在主窗口右侧的列表中。

### 3.2.1.2 Red Flag Server 下 DNS 服务器的安装与配置

#### 1. 打开 DNS 配置工具

打开 DNS 配置工具,必须在 KDE 环境下以 root 权限来运行 DNS 配置工具 rfdns。启动方法有三种:

- (1) 在系统主菜单中选择【系统】|【控制面板】,打开控制面板,在【网络服务配置】选项卡中,双击【DNS 配置工具】;
- (2) 在系统主菜单中选择【管理工具】|【DNS 配置工具】;
- (3) 在运行命令或 shell 提示符下直接输入 rfdns。

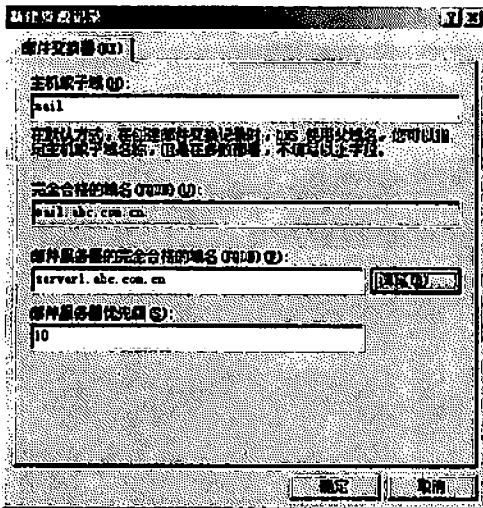


图 3.32 新建邮件交换器

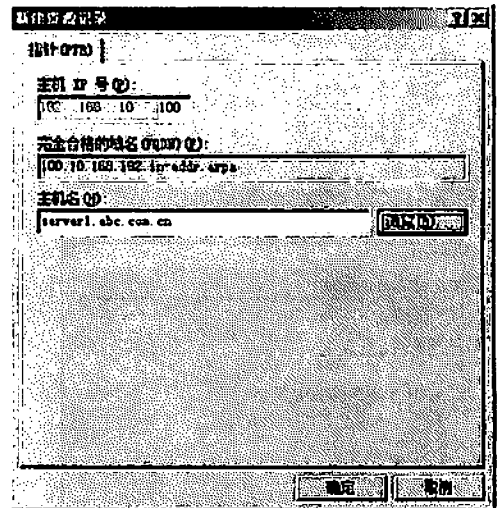


图 3.33 新建指针

#### 2. 启动和停止 DNS 服务

启动、停止和重新启动 DNS 服务可以通过 DNS 配置工具 rfdns,也可以通过命令行终端来完成。

通过 DNS 配置工具 rfdns 来启动、停止和重新启动 DNS 服务的步骤如下:

- (1) 启动 DNS 配置工具 rfdns;
- (2) 在控制台菜单中选择【操作】|【所有任务】,然后选择【启动】命令就可以启动 DNS 服务,选择【停止】命令就可以停止 DNS 服务,选择【重新启动】命令就可以重新启动 DNS 服务。

通过命令行终端来启动、停止和重新启动 DNS 服务的命令如下:



- 启动 DNS 服务: `#/etc/init.d/named start`
- 停止 DNS 服务: `#/etc/init.d/named stop`
- 重新启动 DNS 服务: `#/etc/init.d/named restart`

### 3. Red Flag Server 中添加正向查找区域

(1) 添加正向标准主要区域的步骤如下:

① 在配置工具主窗口左侧的控制台树中, 单击【正向查找区域】。在菜单中选择【操作】|【新建区域】, 弹出【新建区域向导】对话框, 单击【下一步】按钮继续;

② 在出现的【区域类型】界面中, 开始建立一个全新的区域, 选中【标准主要区域】, 单击【下一步】按钮继续;

③ 在出现的【区域名】界面中输入新建区域的名称。如果申请的是一组域名, 比如 `abc.com`, 则只要输入到二级域, 而不是连同子域或主机名称一起输入。单击【下一步】按钮继续;

④ 在出现的【区域文件】界面中, 如果要创建一个新的区域文件, 就直接使用提示的文件名来添加数据。如果这个区域要使用从另一台计算机上复制的文件, 可选中【使用此现存文件】。选择区域文件后单击【下一步】按钮继续;

⑤ 在出现的【正在完成新建区域向导】界面中, 将显示以上步骤所设置的数据列表。如果一切设置正确, 单击【完成】按钮将建立一个正向查找区域, 新建的区域将添加到主窗口的控制台树中。

(2) 添加正向标准辅助区域的步骤如下:

① 添加正向标准辅助区域与添加正向标准主要区域的步骤相同, 在【区域类型】界面中单击【标准辅助区域】, 单击【下一步】按钮继续;

② 在【区域名】界面中为新添加的区域命名后, 单击【下一步】按钮进入【设置复制区域】界面, 设置想要复制区域的服务器。此步骤用来设置想要复制区域的 DNS 服务器源, 可以一次复制多个服务器的数据;

③ 在【IP 地址】中输入可复制的服务器 IP 地址后单击【添加】按钮; 也可以在【服务器名】文本框中输入服务器的主机名后, 单击【解析】按钮获得其 IP 地址再添加;

④ 接着单击【下一步】按钮, 然后依向导提示完成设置。新建的区域将添加到主窗口的控制台树中。

### 4. Red Flag Server 中添加反向查找区域

这里介绍添加反向标准主要区域过程, 添加反向标准辅助区域的过程和添加正向标准辅助区域过程基本相同, 这里就不再介绍了。添加反向标准主要区域步骤如下:

① 在配置工具主窗口左侧的控制台树中, 单击【反向查找区域】。在菜单中选择【操作】|【新建区域】, 弹出【新建区域向导】对话框, 单击【下一步】按钮继续;

② 在出现的【区域类型】对话框中, 开始建立一个全新的区域, 选中【标准主要区域】, 单击【下一步】按钮继续;

③ 在出现的【反向查找区域】界面的【网络 ID】中, 应该以 DNS 服务器 IP 地址的前三段来设置反向查找区域。例如: 我们所使用 DNS 服务器的 IP 地址是 `172.16.82.11`, 则取其前三段即 `172.16.82`。然后, 系统会在【反向查找区域的名称】中, 自动设置为

82.16.172.in-addr.arpa, 单击【下一步】按钮继续;

④ 在出现的【区域文件】界面中, 直接使用默认的文件名即可, 单击【下一步】按钮继续;

⑤ 在出现的【正在完成新建区域向导】界面中, 将显示以上步骤所设置的数据列表。如果一切设置正确, 单击【完成】按钮将建立一个反向查找区域, 新建的区域将添加到主窗口的控制台树中。

#### 5. Red Flag Server 中配置区域属性

##### (1) 修改区域的起始授权机构(SOA)记录

SOA(Start of Authority)用来识别域名中由哪一个名称服务器负责信息授权, 在区域数据库文件中, 第一条记录必须是 SOA 的设置记录。

在配置工具主窗口左侧的控制台树中, 选择相应的区域。单击菜单中的【操作】|【属性】, 也可以右击选择快捷菜单中的【属性】菜单项。打开【区域属性】对话框, 单击【起始授权机构(SOA)】选项卡。

如有需要, 可以修改起始授权机构(SOA)的属性。要调整【刷新闻隔】、【重试间隔】或【过期间隔】, 在下拉列表中选择以秒、分钟、小时、天或星期为单位的时间段, 然后在文本框中键入数字。单击【应用】按钮保存调整后的间隔, 完成更改后单击【确定】按钮使修改生效。

##### (2) 将其他 DNS 服务器指定为区域的权威服务器

在配置工具主窗口左侧的控制台树中选择相应的区域。单击菜单中的【操作】|【属性】, 也可以右击选择快捷菜单中的【属性】菜单项。打开【区域属性】对话框, 单击【名称服务器】选项卡。

如果要向列表中添加名称服务器, 单击【添加】, 即可弹出【新建名称服务器】对话框。按 IP 地址指定其他的 DNS 服务器, 然后单击【添加】将它们加入列表。也可以通过指定服务器 IP 地址或输入其 DNS 名称将区域添加到权威服务器的列表中。输入名称时, 单击【解析】可以在将它添加到列表之前将其名称解析为 IP 地址。

使用该过程指定的 DNS 服务器将被加入到该区域的现有名称服务器(NS)资源记录中。

##### (3) 为辅助区域更新主控服务器

在配置工具主窗口左侧的控制台树中, 选择相应的辅助区域。单击菜单中的【操作】|【属性】, 也可以右击选择快捷菜单中的【属性】菜单项, 打开【区域属性】对话框。

单击【常规】选项卡, 在【IP 地址】中, 为新的主控服务器指定 IP 地址并单击【添加】以便在列表中更新。

#### 6. 管理资源记录

##### (1) 添加主机资源记录

向区域添加主机资源记录的步骤如下:

① 在配置工具主窗口左侧的控制台树中, 选择相应的正向查找区域。单击菜单中的【操作】|【新建主机】, 也可以右击选择快捷菜单中的【新建主机】菜单项。打开【新建主机】窗口。

② 在【名称】文本框中, 填写新增主机记录的名称。不需要填上整个域名, 比如要



新增 sales 名称, 只要输入 sales, 而不是 sales.abc.com;

③ 在【IP 地址】文本框中, 输入新建主机的实际 IP 地址;

④ 单击【添加主机】按钮, 新增的主机记录将显示在主窗口右侧的列表中。重复上述操作可以向区域中添加多个主机资源记录。

#### (2) 添加别名(CNAME)的资源记录

设置别名可以让一个主机拥有多个主机名称。例如, 一个主机当作为 Web 服务器时为 www.abc.com, 而当作为 FTP 服务器时可以是 ftp.abc.com。向区域添加别名(CNAME)的资源记录的步骤如下:

① 在配置工具主窗口左侧的控制台树中, 选择相应的正向查找区域。单击菜单中的【操作】|【新建别名】, 也可以右击选择快捷菜单中的【新建别名】菜单项;

② 在【别名】文本框中, 键入别名。在【目标主机的完全合格的名称】文本框中, 键入使用此别名的 DNS 主机的完全合格域名;

③ 单击【确定】, 完成新增主机别名的操作, 新增的主机别名将出现在主窗口右侧的列表中。

#### (3) 添加邮件交换器(MX)资源记录

向区域添加邮件交换器(MX)资源记录的步骤如下:

① 在配置工具主窗口左侧的控制台树中, 选择相应的正向查找区域。单击菜单中的【操作】|【新建邮件交换器】, 也可以右击选择快捷菜单中的【新建邮件交换器】菜单项;

② 出现新建邮件交换器的界面。在【主机或域】文本框中, 键入使用此记录发送邮件的服务器域名。在【邮件服务器】文本框中, 键入邮件交换器或邮件服务器主机(发送指定域名的邮件)的 DNS 主机名;

③ 若该区域内有多台同样域名的邮件服务器, 可以调整此区域的【邮件服务器优先级】, 数字较小的优先级较高;

④ 单击【确定】, 完成新增邮件交换器的操作, 新增的邮件交换器记录将显示在主窗口右侧的列表中。

#### (4) 添加指针(PTR)资源记录

向反向查找区域添加指针(PTR)资源记录的步骤如下:

① 在配置工具主窗口左侧的控制台树中, 选择适当的反向查找区域。单击菜单中的【操作】|【新建指针】, 也可以右击选择快捷菜单中的【新建指针】菜单项, 弹出新建指针的界面;

② 在【主机 IP 号】文本框中, 键入主机 IP 地址的 8 位字节数。在【主机名】文本框中, 键入 DNS 主机的完全合格域名, 该计算机使用此指针记录提供反向搜索(把 IP 地址解析为域名);

③ 单击【确定】, 建立新增的指针, 新增的指针记录将显示在主窗口右侧的列表中。

#### (5) 修改区域中的现有资源记录

在配置工具主窗口左侧的控制台树中, 单击相应的区域。窗口右侧会显示该区域的详细信息列表, 选择要修改的资源记录项。选择菜单中的【操作】|【属性】, 也可以右击选择快捷菜单中的【属性】菜单项。在相应的属性对话框中, 可以根据需要查看或编辑任何可以修改的属性。

### (6) 从区域中删除资源记录

在配置工具主窗口左侧的控制台树中,单击相应的区域。窗口右侧会显示该区域的详细信息列表,选中要删除的资源记录项。选择菜单中的【操作】|【删除】,也可以右击该项,并在快捷菜单中选择【删除】菜单项。出现提示对话框时,确认是否删除所选的资源记录。

### (7) 使用 rfdns 编辑器

为了使用户能够全面地配置 DNS 服务器支持的全部功能, rfdns 配置工具中提供了一个配置文件编辑器。用户可以通过它直接对 DNS 配置文件进行手工修改(后面将要详细介绍)。在菜单中选择【查看】|【编辑器】,可以切换文件编辑窗口的隐藏与显示。

选中某一区域或资源记录,其对应的配置内容会在配置文件编辑器中被高亮显示出来。对相应配置文件进行编辑后,单击工具栏中的【存储配置文件】按钮。

配置工具也可以检查配置文件的语法错误,检查结果会显示在消息窗口中。如果出现语法错误,请根据提示进行修改。在开始手工修改配置文件后,请不要在存储之前使用配置工具提供的其他配置功能,否则所做的修改将会被覆盖。配置文件修改并存储后,必须重新启动 DNS 服务器才能使修改生效。

## 3.2.1.3 Linux 操作系统下的 DNS 客户端配置文件

每一台 Linux 主机要实现域名解析(不管它是不是域名服务器)都需要配置 DNS 客户端配置文件。Linux 操作系统下的 DNS 客户端配置文件主要有两个,一个是名称转换控制文件,另一个是域名转换程序配置文件。

### 1. 名称转换控制文件

不同的 Linux 中使用不同的名称转换控制文件,在 Red Flag Linux 中使用/etc/nsswitch.conf 文件,而在 Red Hat Linux 中,使用/etc/host.conf 文件。

在 Red Flag Linux 中, /etc/nsswitch.conf 文件用于存放本机主机名以及经常访问 IP 地址的主机名。和域名服务有关的一项是“hosts”。在对 IP 进行域名解析时,可以设定为先访问该文件,再访问 DNS,最后访问 NIS。这一行文件内容如下:

```
hosts: files dns nisplus nis
```

在 Red Hat Linux 中, /etc/host.conf 文件是用来控制转换程序的设置文件。该文件告诉转换程序使用哪些服务及按照什么顺序进行。可以通过“order”来指定,这一行文件内容如下:

```
order hosts,dns,nis
```

在 Red Hat Linux 中,使用/etc/hosts 文件来存放本机主机名以及经常访问 IP 地址的主机名。

### 2. 域名转换程序配置文件

该文件用来设置主机所在域名、域名查找的顺序以及域名服务器的 IP 地址,该配置文件是/etc/resolv.conf。下面是一个域名转换程序配置文件的例子:

```
domain abc.com.cn
```



```
search abc.com.cn xyz.com.cn
nameserver 10.1.14.61
nameserver 10.1.14.62
```

#### 【说明】

(a) domain 用来定义主机的本地域名。

(b) search 用来设置查找域名表。如果要查询的只有主机名称，而不含完整的域名时，会加上这里的域名去查找。如果没设置，就会自动加上 domain 设置的域名。

(c) nameserver 列出域名服务器的 IP 地址。可以设置多个域名服务器，若第一个不能提供服务时就会自动使用第二个。如果 Linux 主机本身就是一台域名服务器，为提高查询速度，应把第一个 nameserver 设置为本地环回地址 127.0.0.1。

### 3.2.1.4 Linux 操作系统下的 DNS 服务器配置文件

在 Linux 操作系统下，有一些和 DNS 服务器配置密切相关的文件，这里作一下简要介绍。下面的例子以一个组织的主域名服务器配置为例，该组织的域名为 abc.com.cn，所使用的网络地址为 210.45.12.0，共有两台服务器，一台的 IP 地址是 210.45.12.100，名字是 a100，它用作域名服务、电子邮件服务，另一台 IP 地址是 210.45.12.101，名字是 a101，它用作 WWW 服务。

#### 1. DNS 服务主配置文件/etc/named.conf

该文件是域名服务器守护进程 named 启动时读取到内存的第一个文件。在该文件中定义了域名服务器的类型、所授权管理的域以及相应数据库文件和其所在的目录。该文件默认的名字是/etc/named.conf。

named.conf 文件的配置一般包括一个全局配置选项(options)部分和多个区(zone)声明部分。

##### (1) 全局配置选项 options

最常用的全局配置选项是定义服务器配置文件的工作目录和转发服务器的 IP 地址。

例如：

```
options {
    directory "/var/named";
    forwarders{
        202.96.134.133;
    };
};
```

#### 【说明】

(a) directory 指定了 DNS 数据文件的存放目录是/var/named。

(b) forwarders {202.96.134.133;}，其中 202.96.134.133 是转发 DNS 服务器的地址，forwarders 参数指定其后的 IP 所在的服务器作为备选的 DNS 服务器。也就是说，把本机 DNS 不能解析的主机发送到这个备选的 DNS 服务器上，让它来进行解析。

##### (2) 区(zone)声明

区声明是配置文件中最重要的一部分，可有多个区声明，每一条区声明需要说明域名、

服务器的类型和域信息源三项。例如：

```
zone "abc.com.cn" IN {  
    type master;  
    file "named.hosts";  
    notify no;  
};
```

#### 【说明】

(a) zone "abc.com.cn" 用于定义这个区的名称。

(b) type 指定服务器类型。可选的类型的 master, slave 和 hint。master 说明一个区的主域名服务器；slave 说明一个区的辅助域名服务器；hint 说明一个区的高速缓存文件。可以通过该参数来说明这台服务器是主域名服务器、辅助域名服务器或缓存域名服务器。

(c) file 指明该区资源记录存放的文件名称。

(d) notify 用来设置是否自动发出 DNS NOTIFY 信息，其预设值为 yes，也就是当主域名服务器中数据库文件发生修改时，自动发出 DNS NOTIFY 信息，当辅助域名服务器收到这个信息后就自动向主域名服务器确认是否需要更新资料，并自动更新。

#### ① 根域名区声明

该区用来告诉域名服务器的守护程序必须维护一个高速缓存域名服务器，同时还告诉域名服务器的守护程序利用什么文件去初始化高速缓存，其类型必须设置为 hint，该文件一般存放在 named.ca 中。例如：

```
zone "." IN {  
    type hint;  
    file "named.ca";  
};
```

#### ② 反向环回地址区声明

反向环回地址区主要设置环回地址反向解析文件的位置，其内容如下：

```
zone "0.0.127.in-addr.arpa" IN {  
    type master;  
    file "named.local";  
    allow-update { none; };  
};
```

#### ③ 正向域名解析区声明

正向域名解析区主要是设置本区域正向域名解析数据文件。若该 DNS 服务器是一个缓存域名服务器，则不需要配置该区。若该 DNS 服务器是一个主域名服务器，则 type 指定为 master。下面的例子是一个主域名服务器，其域名为“abc.com.cn”，正向域名解析数据存放在 named.hosts 文件之中。

```
zone " abc.com.cn " IN {  
    type master;  
    file " named.hosts";  
    allow-update { none; };
```

```
};
```

如果是辅助域名服务器,则 type 指定为 slave,同时还要指定主域名服务器的 IP 地址,以便进行数据库更新,其格式为 masters{<主域名服务器的 IP 地址>}。例如主域名服务器地址为 210.45.12.101,则内容如下:

```
zone " abc.com.cn " IN {  
type slave;  
file "named.hosts";  
masters{210.45.12.101}  
};
```

#### ④ 反向域名解析区声明

反向域名解析区主要是设置本区域反向域名解析数据文件。若该 DNS 服务器是一个缓存域名服务器,也不需要配置该区;若该 DNS 服务器是一个主域名服务器,则 type 指定为 master。下面的例子是一个主域名服务器,它负责 210.45.12.0 网络的反向解析,反向域名解析数据存放在 named.rev 文件之中。

```
zone "12.45.210.in-addr.arpa" IN {  
type master;  
file "named.rev";  
allow-update { none; };  
};
```

如果是辅助域名服务器,则 type 指定为 slave,同时还要指定主域名服务器的 IP 地址,以便进行数据库更新,其格式为 masters{<主域名服务器的 IP 地址>}。例如主域名服务器地址为 210.45.12.101,则内容如下:

```
zone "12.45.210.in-addr.arpa" IN {  
type slave;  
file "named.rev";  
masters{210.45.12.101}  
};
```

## 2. DNS 的数据库文件和资源记录

### (1) 资源记录

在/etc/named.conf 文件中所定义的文件都是 DNS 数据库文件(如本例中 named.ca、named.local、named.hosts、named.rev),每个文件都由资源记录构成。每条资源记录包含与特定主机的有关信息。而每一条资源记录通常包含 5 项,按一行记录在文本文件之中,其格式如下:

[域名] [存活期 ttl] IN <记录类型> <记录数据>

- (a) 域名:给出要定义的资源域名,该域名通常用来作为域名查询时的关键字。
- (b) 存活期:在存活期内,该记录有效,存活期过后,该记录不再有效。
- (c) IN:将记录标识为一个 Internet DNS 资源记录。
- (d) 记录类型:该项表明资源记录的类型,下面将详细介绍。

(e) 记录数据: 说明和该资源记录相关的信息, 通常由资源记录类型来决定。

资源记录主要有以下几种类型:

- 主机(A)记录: 用来记录在正向查找区域内的主机及其 IP 地址, 用户可通过该类型的资源记录把主机域名映射成 IP 地址。
- 主机别名(CNAME)记录: 在某些情况下, 需要为区域内的一台主机创建多个主机名称, 例如, 一台主机同时是 Web 服务器与 FTP 服务器, 则可以为该主机取两个不同名称, 当作 Web 服务器时域名为“www.abc.com”, 而当作 FTP 服务器时域名可以是“ftp.abc.com”。
- 邮件交换器(MX)记录: 当用户将邮件送到本地邮件服务器后, 本地邮件服务器必须将邮件送到目的地邮件服务器, 而目的地的邮件服务器 IP 地址可以向 DNS 服务器查询。邮件交换器记录就是指定哪些主机负责接收该区域的电子邮件, 如果在此区域内创建了多个邮件交换器记录, 可以调整此区域邮件服务器的优先级, 数字较低的优先级较高。
- 指针(PTR)资源记录: 用来记录在反向查找区域内的 IP 地址及主机, 用户可通过该类型的资源记录把 IP 地址映射成主机域名。
- 起始授权机构(SOA)记录: 起始授权机构用来记录此区域中的主要名称服务器以及管理此 DNS 服务器的管理员的电子邮件信箱。
- 名称服务器(NS)记录: 名称服务器记录用来记录管辖此区域的名称服务器, 包括主域名服务器和辅助域名服务器。

## (2) 高速缓存初始化文件

在 Linux 系统上通常在/var/named 目录下已经提供了一个 named.ca, 该文件中包含了 Internet 的顶层域名服务器, 但这个文件通常会有变化, 所以建议最好从 Inter NIC 下载最新的版本。该文件可以通过匿名 ftp 下载。

## (3) 环回地址转换文件

该文件用来说明“环回地址”的 IP 地址到主机名的映射。其文件名由/etc/named.conf 中反向环回地址区定义, 通常为/var/named/named.local, 该文件的内容如下:

```
$TTL 86400
@      IN  SOA      localhost. root. localhost. (
                                2001110600 ;    serial
                                28800       ;refresh
                                14400       ;retry
                                3600000    ;expire
                                86400      ) ;minimum
      IN  NS       localhost.
1      IN  PTR     localhost.
```

### 【说明】

(a) 此文件的内容是特定的, 在不同的域的域名服务器上, 所要修改的只是 SOA 记录和 NS 记录。

(b) “PTR”记录的最后域名为完全标识域名, 以“.”结束。



#### (4) 正向域名转换数据文件

该文件指定了域中主机域名同 IP 地址的映射, 实现域名的正向解析。其文件名由 `/etc/named.conf` 中正向域名解析区声明定义, 本例中该文件名为 `/var/named/named.hosts`。其内容如下:

```
STTL 86400
@      IN  SOA      a100.abc.com.cn.  root.abc.com.cn. (
                        2001110600 ; serial
                        28800 ; refresh
                        14400 ; retry
                        3600000 ; expire
                        86400 ; minimum
                        )
      IN  NS  a100.abc.com.cn.
      IN  MX  10 a100.abc.com.cn.
localhost. IN  A   127.0.0.1
a100      IN  A   210.45.12.100
a101      IN  A   210.45.12.101
www       IN  CNAME a101
```

#### 【说明】

- (a) 在文件中所有的记录行都要顶格写, 前面不能有空格。
- (b) 行 “IN NS a100.abc.com.cn.” 说明该域的域名服务器, 至少应该定义一个。
- (c) 行 “IN MX 10 a100.abc.com.cn.” 是一条邮件交换器(MX)记录, 指明了单位的邮件交换器是 a100.abc.com.cn, 它负责处理邮件地址的主机部分为 “@abc.com.cn” 的邮件, “10” 表示优先级别。
- (d) 类似于行 “a100 IN A 210.45.12.100” 的是一系列的 A 记录, 表示主机名和 IP 地址的对应关系。a100 是主机名, 210.45.12.100 是它的 IP 地址。
- (e) 行 “www IN CNAME a101” 表示一条定义别名的记录。即 “www.abc.com.cn” 和 “a101.abc.com.cn” 表示同一台主机。

#### (5) 反向域名转换数据文件

该文件主要定义了 IP 地址到主机名的转换, 实现域名的反向解析。IP 地址到主机名的转换是非常重要的, Internet 上的很多应用, 例如 NFS、Web 服务等都要用到该功能。其文件名由 `/etc/named.conf` 中反向域名解析区声明定义, 本例中其名称为 `/var/named/named.rev`。该文件的内容如下:

```
STTL 86400
@      IN  SOA      a100. abc.com.cn.  root. abc.com.cn. (
                        2001110600 ; serial
                        28800 ; refresh
                        14400 ; retry
                        3600000 ; expire
                        86400 ; minimum
                        )
```

```
      IN  NS      abc.com.cn.
100   IN  PTR     a100.abc.com.cn.
101   IN  PTR     a101.abc.com.cn.
```

### 【说明】

(a) PTR 记录用于定义 IP 地址名到主机域名的映射。即 IP 地址 210.45.12.100 对应的主机名为 a100.abc.com.cn, IP 地址 210.45.12.101 对应的主机名为 a101.abc.com.cn。

(b) PTR 记录的最后一项必须是一个完整的标识域名, 以 “.” 结束。

注: 在辅助域名服务器和缓存域名服务器中, 不需要配置正向域名转换数据文件 /var/named/named.hosts 和反向域名转换数据文件 /var/named/named.rev。但在辅助域名服务器中, 若不存在这两个文件, 域名服务器的守护程序将自动从主域名服务器中下载这两个文件, 文件内容与主域名服务器完全相同; 若文件存在, 则检查主域名服务器中的数据是否不同于本地文件, 若有变化, 就下载并更新本地文件的内容; 若无变化, 就加载本地磁盘文件, 不必从远程下载。

### 3. 启动、停止和重新启动域名服务器

默认安装时, 域名服务器的守护程序为 /etc/rc.d/init.d/named, 是域名服务的最主要文件。用户可以通过该程序启动、重新启动、停止域名服务, 命令分别是:

```
#/etc/rc.d/init.d/named start
#/etc/rc.d/init.d/named restart
#/etc/rc.d/init.d/named stop
```

如果设定 DNS 服务在计算机启动时自动启动或不启动, 可以通过 chkconfig 命令来设定, 该命令格式是:

```
chkconfig [--level <运行级>] <名字> [on|off]
```

例如, 我们希望计算机在运行级别 3、5 的情形下启动时自动启动 DNS 服务, 则命令为:

```
#chkconfig --level 35 named on
```

再如, 我们希望计算机在运行级别 2 的情形下启动时不启动 DNS 服务, 则命令为:

```
#chkconfig --level 2 named off
```

## 3.2.2 典型例题分析

例 1 阅读以下说明, 回答问题 1~5, 将解答填入对应的答案栏内。

### 【说明】

某公司在国际网互联中心申请了一个 C 类的 IP 地址 210.45.12.0/24, 域名为 abc.com.cn。该公司有一台该 Web 服务器(IP 地址为 210.45.12.11, 主机名为 S1), 一台 FTP 服务器(IP 地址为 210.45.12.12, 主机名为 S2)、一台 MAIL 服务器 (IP 地址为 210.45.12.13, 主机名为 S3)和一台 DNS 服务器(IP 地址为 210.45.12.14, 主机名为 S4)。若你是该公司的网络管

理员,使用一台装有 Windows Server 2003 服务器作为 DNS 服务器。

【问题 1】该服务器必须是什么类型的 DNS 服务器?

【问题 2】该 DNS 服务器的正向查找区域是什么?反向查找区域是什么?

【问题 3】现已在正向查找区域中添加了一些主机记录,当用户的浏览器地址栏中输入“http://sl.abc.com.cn”时可以访问该公司的主页,但输入“http://www.abc.com.cn”时却不能访问该公司的主页,问题出在哪儿?如何解决?

【问题 4】原来该公司用户的电子邮件地址格式是“xxx@mail.abc.com.cn”,现在想把它改为“xxx@abc.com.cn”。除了在邮件服务器上作修改之外,在域名服务器上还要做哪些修改?

【问题 5】现在反向查找区域添加了一个指针(PTR)记录,该记录的作用是什么?

分析:该题主要考查考生对 Windows Server 2003 下 DNS 服务器配置的掌握情况。

问题 1:由于该区域只有一台 DNS 服务器,因此该服务器必须被配置为主域名服务器。在创建时,区域类型必须选择“主要区域”。

问题 2:正向查找区域可以让 DNS 客户端利用主机的域名查询其 IP 地址,反向查找区域可以让 DNS 客户端利用 IP 地址查询主机的域名。因此该服务器必须负责域 abc.com.cn 的正向解析,负责 210.45.12.0/24 这一网络的反向解析。反向域名有两部分组成,域名前半段是其网络 ID 反向书写,而区域后半段必须是“in-addr.arpa”。因此域名为 12.45.210.in-addr.arpa。

问题 3:为了使一台主机有多个主机名称,通常使用别名资源记录(CNAME)。题中已能实现对 sl.abc.com.cn 的解析,说明已经有该服务的主机记录(A),要使其也能解析 www.abc.com.cn,则要添加一条别名资源记录(CNAME),别名为 www.abc.com.cn,真实主机名为 sl.abc.com.cn。

问题 4:邮件服务器的地址、邮件地址格式和多台邮件服务器的优先级可通过邮件交换器(MX)记录指定,邮件地址格式可通过“主机名或域”来定义。因此,可以先删除这一记录,再添加一条邮件交换器(MX)记录,但“主机或域名”处不要填写任何内容。

问题 5:反向查找区域可以让 DNS 客户端利用 IP 地址查询主机的域名,因此作用是实现 IP 地址向域名的映射。

答案:

【问题 1】主域名服务器

【问题 2】abc.com.cn、12.45.210.in-addr.arpa

【问题 3】可能是没有将 sl.abc.com.cn 的别名设置为 www.abc.com.cn,或者设置不正确。可以在正向查找区域中增加一条别名(CNAME)记录,使真实主机名为 sl.abc.com.cn,别名为 www.abc.com.cn。

【问题 4】在正向查找区域中,删除原有的邮件交换器记录(MX),新建一条邮件交换器记录(MX),在“主机或域名”处不要填写任何内容,服务器地址设置为“s3.abc.com.cn”。

【问题 5】实现 IP 地址向域名的映射。

例 2 阅读以下说明,回答问题 1~6,将解答填入对应的答案栏内。

【说明】

某公司的域名为 xyz.edu.cn, 所使用的网络地址为 222.78.68.0/24, 共有两台服务器, 一台的 IP 地址是 222.78.68.10, 名字是 server1, 它用作域名服务器、电子邮件(MAIL)服务器, 另一台 IP 地址是 222.78.68.11, 名字是 server2, 它用作 WWW 服务。下面是该公司 server1 中的 3 个文件。

● /etc/named.conf 文件的内容:

```
options {
directory "/var/named";
};
zone "." IN {
type (1);
file "named.ca";
};
zone "0.0.127.in-addr.arpa" IN {
type master;
file "named.local";
allow-update { none; };
};
zone " xyz.edu.cn " IN {
type master;
file " named.hosts";
allow-update { none; };
};
zone " (2) " IN {
type master;
file "named.rev";
allow-update { none; };
};
```

● /var/named/named.hosts 文件的内容:

```
$TTL 86400
@      IN  SOA      server1.xyz.edu.cn. root.xyz.edu.cn. (
                                2001110600 ; serial
                                28800 ; refresh
                                14400 ; retry
                                3600000 ; expire
                                86400 ; minimum
                                )
      IN  NS  server1.xyz.edu.cn.
      IN  MX  10  server1.xyz.edu.cn.
localhost. IN  A    127.0.0.1
server1    IN  A    222.78.68.10
server2    IN  A    222.78.68.11
www        IN  A    (3)
```



- /var/named/named.rev 文件的内容:

```
$TTL 86400
@      IN  SOA      server1. xyz.edu.cn.  root.xyz.edu.cn. (
        2001110600 ; serial
        28800 ; refresh
        14400 ; retry
        3600000 ; expire
        86400 ; minimum
        )
        IN  NS  xyz.edu.cn.
10      IN  (4)
11      IN  PTR server2.xyz.edu.cn.
```

【问题 1】该服务器是一个什么类型的域名服务器?

【问题 2】(1)处应当填写什么内容?

【问题 3】(2)处应当填写什么内容?

【问题 4】(3)处应当填写什么内容?

【问题 5】(4)处应当填写什么内容?

【问题 6】/var/named/named.hosts 文件中阴影一行的含义是什么?

分析: 该题主要考查考生对 Linux 下 DNS 服务器配置的掌握情况。

该例中共列出 3 个文件, 第一个文件是 DNS 服务主配置文件, DNS 守护进程 named 启动时读取到内存的第一个文件。在该文件中定义了域名服务器的类型、所授权管理的域以及相应数据库文件和其所在的目录。该文件内容包括一个全局配置选项(options)部分和多个区(zone)声明部分。第二个文件是正向域名转换数据文件, 该文件指定了域中主机域名向 IP 地址的映射, 实现域名的正向解析。第三个文件是反向域名转换数据文件, 该文件主要定义了 IP 地址到主机名的转换, 实现域名的反向解析。

问题 1: 可以用 type 来指定服务器类型, 可以通过它来说明这台服务器是主域名服务器、辅助域名服务器或缓存域名服务器。master 说明一个区的主域名服务器; hint 说明一个区的高速缓存文件; slave 说明一个区的辅助域名服务器。本例中的正向域名解析区声明和反向域名解析区声明中都指明了 type 为 master, 则这台服务器是主域名服务器。

问题 2: 不管是主域名服务器、辅助域名服务器还是缓存域名服务器, 在根域名区声明时, type 类型必须为 hint, 即为一个区的高速缓存文件, 因此(1)处应当填写“hint”。

问题 3: (2)处所在位置是反向域名解析区声明, 应当填写反向域名。反向域名由两部分组成, 域名前半段是其网络 ID 反向书写, 而区域后半段必须是“in-addr.arpa”。因此(2)处应当填写“68.78.222.in-addr.arpa”。

问题 4: (3)处应当是一条定义别名的记录。根据说明, 该单位的 www 服务 server2 上, 即“www.xyz.edu.cn”和“server2.xyz.edu.cn”表示同一台主机。因此(3)处应当填写“IN CNAME server2.xyz.edu.cn.”, 也可以只填写“IN CNAME server2”。(注: 此处若要填写“A 222.78.68.11”也可实现解析, 但违背出题的初衷了。)

问题 5: (4)处应当填写一条解析指针(PTR)资源记录: 用来记录在反向查找区域内的 IP 地址及主机, 用户可通过该类型的资源记录把 IP 地址映射成主机域名。此处应当填写“PTR

server1.xyz.edu.cn.”。

问题 6: 阴影的一行是一条邮件交换器(MX)记录, 指定哪些主机负责接收该区域的电子邮件。此处作用是指明了该单位的邮件交换器是 server1.xyz.edu.cn, 它负责处理邮件地址的主机部分为“@xyz.edu.cn”的邮件, “10”表示优先级别。

答案:

【问题 1】主域名服务器

【问题 2】hint

【问题 3】68.78.222.in-addr.arpa

【问题 4】IN CNAME server2.xyz.edu.cn.或者 IN CNAME server2

【问题 5】PTR server1.xyz.edu.cn.

【问题 6】指明了该单位的邮件交换器是 server1.xyz.edu.cn, 它负责处理邮件地址的主机部分为“@xyz.edu.cn”的邮件, “10”表示优先级别。

例 3 回答问题 1~4, 将解答填入对应的答案栏内。

【问题 1】DNS 的作用是什么?

【问题 2】Internet 中的域名是如何组织的?

【问题 3】Internet 域名解析有哪两种方式?

【问题 4】以域名 www.cs.pku.edu.cn 为例, 说明域名系统是如何进行域名解析的。

分析: 该题主要考察考生对 DNS 服务的基本概念的理解。

DNS 域名系统基础已在《网络管理员考试同步辅导(计算机与网络基础知识篇)》第 5 章中作了详细介绍, 读者可参阅此书。

问题 1: 域名系统(DNS)就是实现 IP 地址和域名之间的映射。

问题 2: Internet 的域名是具有一定层次的树状结构。它实际上是一个倒置的树, 树根在最上面。Internet 将所有联网的主机的域名空间划分为许多不同的域, 树根是最高一级域。每一个最高级的域又被分成一系列的二级域。三级域和更低级域又是二级域的分支。

问题 3: 将域名映射为 IP 地址或将 IP 地址映射成域名, 都称为域名解析。DNS 被设计为客户端/服务器应用程序。域名解析可以有两种方式:

第一种叫递归解析, 要求域名服务器系统一次性完成全部域名和地址之间的映射。换句话说, 解析程序期望服务器提供最终解答, 若服务器是该域名的授权服务器, 就检查其数据库并响应; 若服务器不是授权服务器, 该服务器就将请求发送给另一个服务器并等待响应, 直到查找到该域名授权服务器, 并把响应的结果发送给请求的客户。

第二种叫迭代解析, 每一次请求一个服务器, 不行再请求别的服务器。换言之, 若服务器是该域名的授权服务器, 就检查其数据库并响应, 完成解析; 若不是, 就返回认为可以解析这个查询的服务器的 IP 地址。客户就向第二服务器重复查询, 若新找到的服务器能解决这个问题, 就响应并完成解析; 否则, 就向客户返回一个新服务器的 IP 地址。客户如此重复同样的查询, 直到找到该域名的授权服务器。

问题 4: 域名 www.cs.pku.edu.cn 的解析过程(以迭代解析为例, 若给出递归解析过程也正确):

(1) 本地域名服务器收到域名解析的请求后, 查找其缓存内的域名信息。若缓存中有

主机域名或 IP 地址, 则返回给用户。反之则向其他 DNS 服务器查询。

(2) 根 DNS 服务器返回它所知道的最佳结果, 如: .cn 域名服务器的域名与 IP 地址。

(3) 本地 DNS 服务器向 .cn 服务器发出查询请求, .cn 域名服务器返回 edu.cn 域名服务器的 IP 地址。

(4) 本地 DNS 服务器向 edu.cn 域名服务器发出查询请求, edu.cn 域名服务器返回 pku.edu.cn 的 IP 地址。

(5) 本地 DNS 服务器向 pku.edu.cn 域名服务器发出查询请求, pku.edu.cn 域名服务器返回 cs.pku.edu.cn 的 IP 地址。

(6) 本地 DNS 服务器将该查询结果返回给客户。

答案:

【问题 1】DNS 的作用是将符号化的域名映射为 IP 地址

【问题 2】Internet 中的域名是按树形结构组织的

【问题 3】Internet 域名解析有递归解析和迭代解析两种方式

【问题 4】略

### 3.2.3 同步练习

1. 在 Red Flag Linux 中可以通过什么命令启动 DNS 配置工具?
2. 在 Red Flag Linux 中如何通过启动 DNS 服务? 请说出两种方法。
3. 在 Red Flag Linux 的 DNS 配置工具中编辑器的功能是什么?
4. 阅读以下说明, 回答问题 1~问题 5, 将解答填入对应的答案栏内。

【说明】

下面是某公司一台 Linux 中/etc/named.conf 文件的内容:

```
options {  
    directory "/var/named";  
};  
  
zone "." IN {  
    type hint;  
    file "named.ca";  
};  
  
zone "0.0.127.in-addr.arpa" IN {  
    type master;  
    file "named.local";  
    allow-update { none; };  
};  
  
zone " abc.com.cn " IN {  
    type slave;  
    file " named.hosts";  
    masters{210.45.12.101}  
};  
  
zone "12.45.210.in-addr.arpa" IN {
```

```
type slave;  
file "named.rev";  
masters(210.45.12.101)  
};
```

【问题 1】该服务器负责的正向解析的区域是什么？能实现哪个网络的 IP 地址的反向解析？

【问题 2】该服务器是一个什么类型的域名服务器？

【问题 3】该域名服务器的数据文件的存放目录是什么？

【问题 4】文件中“file “named.ca”；”一行的含义是什么？

【问题 5】文件中“masters(210.45.12.101)”的含义是什么？

### 3.2.4 同步练习参考答案

1. 在 KDE 环境下以 root 权限来运行 DNS 配置工具 rfdns。
2. 方法一：使用命令行终端来启动，命令如下：

```
#/etc/init.d/named start
```

方法二：通过 DNS 配置工具 rfdns 来启动：启动 DNS 配置工具 rfdns，在控制台菜单中选择【操作】|【所有任务】，然后选择【启动】命令。

3. DNS 配置工具中编辑器的功能使得用户可以手工修改 DNS 的配置文件。
- 4.

【问题 1】abc.com.cn、210.45.12.0/24

【问题 2】辅助域名服务器(从域名服务器)

【问题 3】/var/named

【问题 4】告诉域名服务器守护程序利用/var/named/named.ca 文件去初始化高速缓存

【问题 5】该区域的主域名服务器的 IP 地址是 210.45.12.101

## 3.3 电子邮件服务

### 3.3.1 考点辅导

#### 3.3.1.1 Windows Server 2003 下电子邮件服务器的安装与配置

我们可以通过 Windows Server 2003 提供的 POP3 服务和 SMTP 服务架设小型邮件服务器来满足需要。

##### 1. 电子邮件服务器的安装

(1) 选择【开始】|【管理工具】|【管理您的服务器】，将出现服务器管理窗口，单击【添加或删除角色】连接，单击【下一步】按钮，系统显示【服务器角色】界面，选中【邮件服务器(POP3, SMTP)】，如图 3.34 所示。



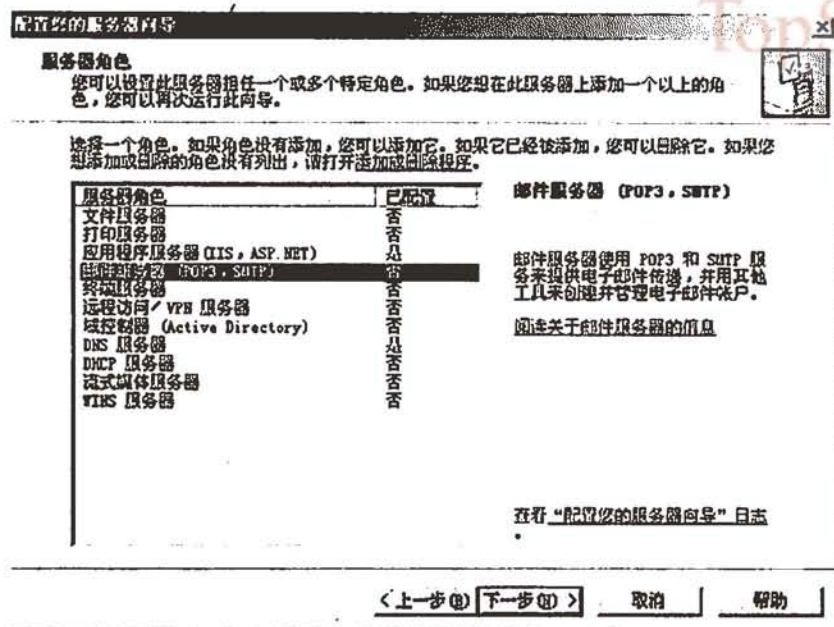


图 3.34 选择【服务器角色】界面

(2) 单击【下一步】按钮，弹出【配置 POP3 服务】界面，其中包括选择身份验证方法和输入电子邮件域名两部分。身份验证方法包括本地 Windows 账户身份验证和加密密码文件两种验证方式。选择身份验证方式、输入电子邮件域名，如图 3.35 所示。

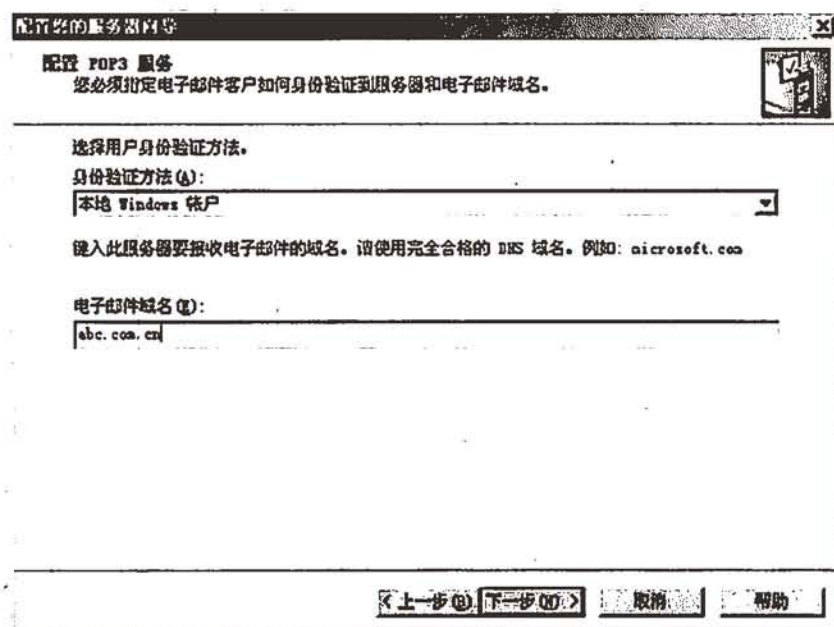


图 3.35 【配置 POP3 服务】界面

(3) 单击【下一步】按钮，显示【选择总结】界面，如图 3.36 所示。

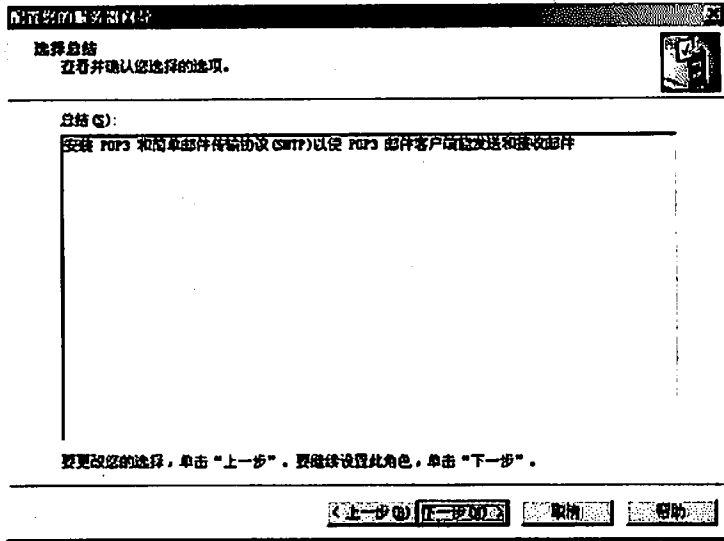


图 3.36 【选择总结】界面

- (4) 确认选择后, 单击【下一步】按钮, 按照系统提示插入光盘, 如图 3.37 所示。

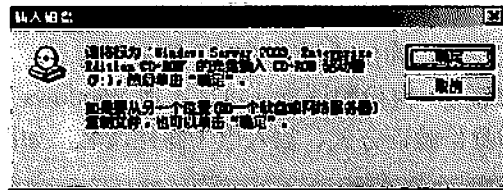


图 3.37 【插入磁盘】界面

- (5) 系统自动进行电子邮件服务组件的安装, 如图 3.38 所示。

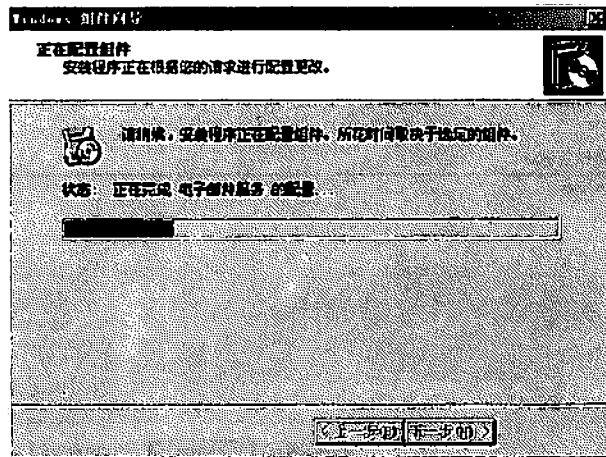


图 3.38 系统正在安装邮件服务器

- (6) 安装完毕后, 系统提示此服务器已经是邮件服务器, 如图 3.39 所示。单击【完成】按钮后, 邮件服务器就出现在【管理您的服务器】窗口中。

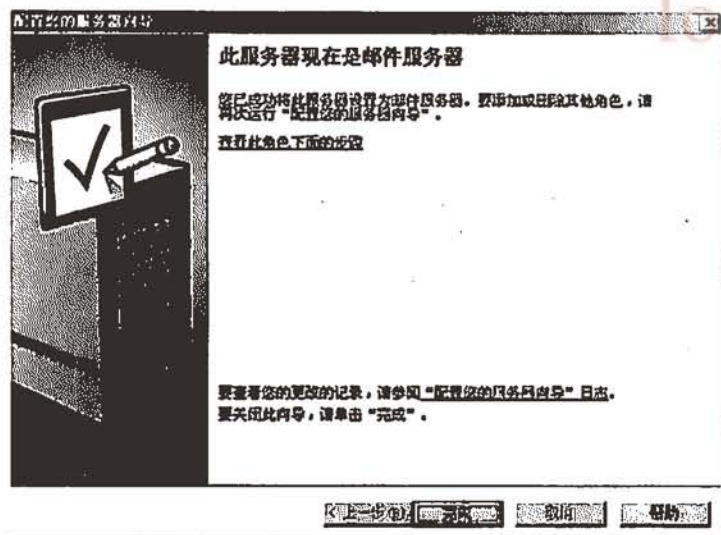


图 3.39 邮件服务器安装完成

## 2. 邮箱存储位置设置

安装完成后，默认状态下系统将用户邮件存储在 C:\inetpub\mailroot\Mailbox 文件夹中，通常需要将邮件的存储地址修改到一个空间比较大的存储位置，但要进行这样的修改需要有足够的权限，要由 Administrators 组中的成员来进行修改。设置邮件存储位置的操作如下：

(1) 在【管理您的服务器】窗口中单击【邮件服务器(POP3, SMTP)】中的【管理此邮件服务器】，系统显示【POP3 服务】控制台，如图 3.40 所示。

(2) 首先停止邮件服务器。右击【POP3 服务】下的计算机名称，在弹出的快捷菜单中选择【所有任务】|【停止】。

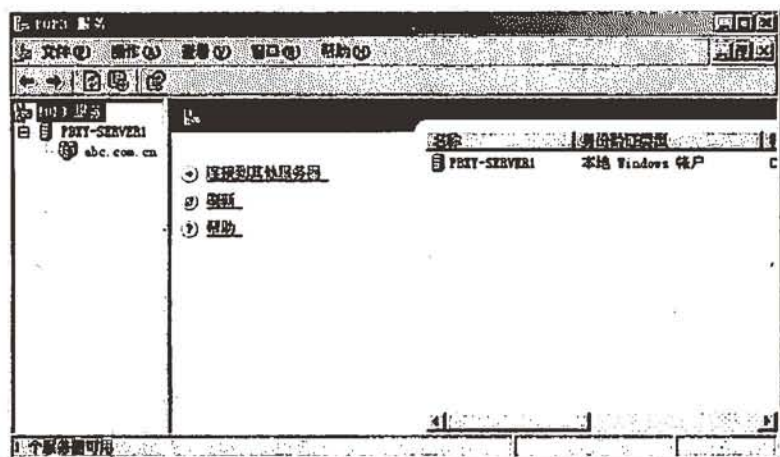


图 3.40 【POP3 服务】控制台

(3) 右击【POP3 服务】下的计算机名称，在弹出的快捷菜单中选择【属性】菜单，系统显示邮件服务器的属性对话框，在【根邮件目录】文本框中输入邮件存储文件夹，或单击【浏览】按钮，选择邮件存储文件夹，如图 3.41 所示。

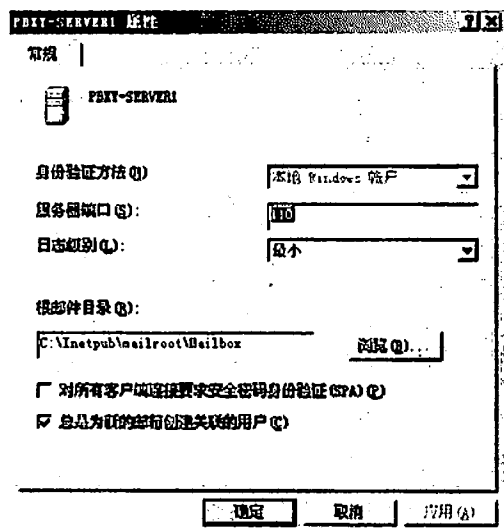


图 3.41 邮件服务器属性框

(4) 单击【确定】按钮，系统提示用户原有域无法存储邮件，需将域目录复制到新目录下，单击【确定】按钮，如图 3.42 所示。

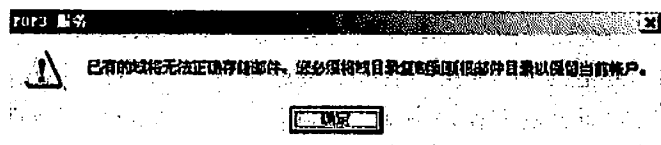


图 3.42 配置邮件服务器提示(一)

(5) 系统提示重启邮件服务器，单击【是】按钮，如图 3.43 所示。

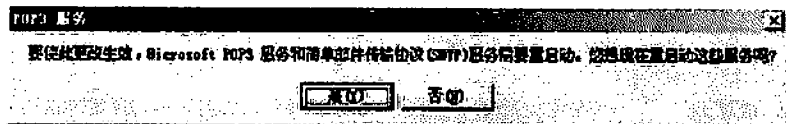


图 3.43 配置邮件服务器提示(二)

(6) 将系统默认状态下邮件存储文件夹，例如 C:\inetpub\mailroot\Mailbox 中的域复制到新的邮件存储文件夹。

(7) 右击【POP3 服务】下的计算机名称，在弹出的快捷菜单中选择【所有任务】|【重新启动】，启动邮件服务。

(8) 右击【POP3 服务】下的计算机名称，在弹出的快捷菜单中选择【刷新】，使新的域目录生效。

### 3. 域管理

邮件服务器中通过域来提供邮件服务。如果一个企业或单位需要多个域名，可以添加多个域名实现多邮件虚拟服务共享。

#### (1) 创建域

① 打开【POP3 服务】控制台，右击计算机名称，在弹出的快捷菜单中选择【新建】|



【域】，系统显示【添加域】。

② 在域名文本框中输入新建域的名称，如图 3.44 所示，并确保该域名已在 DNS 服务器中设置好 MX 记录。

③ 单击【确定】按钮，完成新域的添加。

#### (2) 删除域

打开【POP3 服务】控制台，右击要删除的域，单击【删除】按钮，然后单击【确定】按钮，即可删除该域。但是，若该域中有用户正连接到服务器，不能删除该域。

#### (3) 锁定/解除锁定域

通过锁定某个域，可阻止该域的其他成员检索自己的电子邮件。

打开【POP3 服务】控制台，右击要锁定的域，即可锁定该域；同样右击要解除锁定的域，即可解除该域锁定。

### 4. 邮箱管理

#### (1) 新建邮箱

在【POP3 服务】控制台选项中，选中要创建新邮箱的域，右击并在弹出的快捷菜单中选择【新建】|【邮箱】，即可出现【添加邮箱】对话框，分别在【邮箱名】、【密码】、【确认密码】的文本框中，输入相应内容，单击【确定】按钮，系统提示成功添加了一个名为 zhang 的邮箱，如图 3.45 所示。



图 3.44 【添加域】对话框

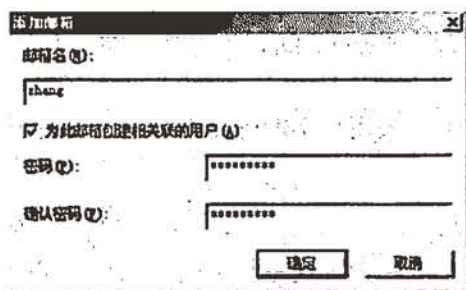


图 3.45 【添加邮箱】对话框

如图 3.46 所示，在名为 PBXY-SERVER1 的服务器上，创建了 abc.com.cn 域，在该域中创建了三个邮箱，分别是 zhang@abc.com.cn、taoan@abc.com.cn 和 liwenlong@abc.com.cn。

#### (2) 删除邮箱

首先在域中右击欲删除的邮箱，然后在弹出的快捷菜单中单击【删除】命令，系统显示【删除邮箱】对话框。若同时删除与此邮箱相关联的用户账户则选中该复选框，单击【确定】按钮即可删除该邮箱。

此外，用户还可以根据需要进行邮箱的锁定、邮箱属性设置等邮箱的管理操作。

### 3.3.1.2 Linux 下电子邮件服务器的安装与配置

Linux 下电子邮件服务器的安装与配置主要包括两个服务器的安装与配置。一个是电子邮件传输服务器 SendMail 的安装与配置；另一个是电子邮件阅读服务器 POP3 和 IMAP 的安装和配置。下面将分别介绍这两个服务器的安装和配置过程。

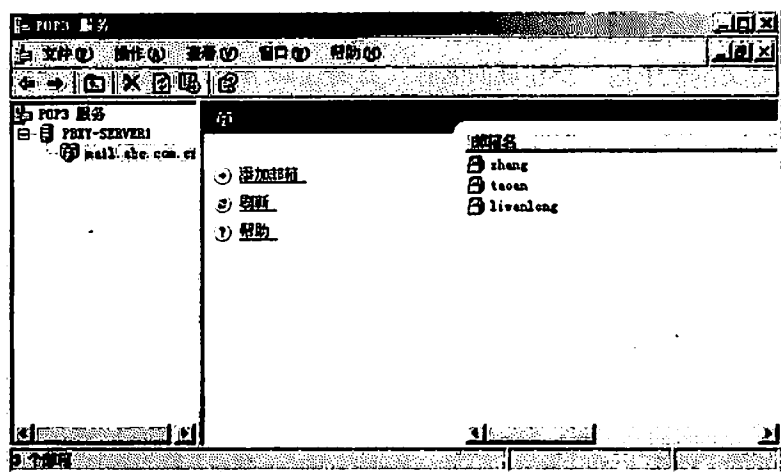


图 3.46 POP3 服务器配置结果

### 1. 电子邮件传输服务器 SendMail 的安装与配置

SendMail 是一个使用最广泛的电子邮件传输服务器 MTA。其历史可从 APARNET 时候开始。简单地说, Sendmail 的功能就是以 SMTP 传送邮件以及接收邮件为主要功能的服务器。Sendmail 的程序非常复杂, 设置复杂而功能强大, 很多邮件服务器都使用 Sendmail。下面以 Red Hat Linux 7.0 为例, 介绍电子邮件传输服务器 SendMail 的安装与配置。

#### (1) Sendmail 的安装

由于 Red Hat Linux 7.0 已内置了 Sendmail, 因此用户在安装 Linux 时, 就不需要另行安装。如果用户不能确定是否已经安装了 Sendmail, 则可以执行以下命令检查:

```
#rpm -qa |grep sendmail
sendmail-8.11.6-3 //若出现此行, 则表示已经安装了 Sendmail, “8.11.6-3”为版本号
```

如果用户发现系统未安装 Sendmail, 则可以在网上下载 Sendmail 安装包。也可以在 Red Hat Linux 安装盘中找到 Sendmail 安装包。一般来说需要安装以下 3 个安装包: 主程序包、可供参考使用的配置文件、说明文档。安装命令如下:

```
#rpm -ivh sendmail-8.11.6-3.i386.rpm //安装主程序包
#rpm -ivh sendmail-cf-8.11.6-3.i386.rpm //安装可供参考使用的配置文件
#rpm -ivh sendmail-doc-8.11.6-3.i386.rpm //安装说明文档
```

如果用户想从旧版本的 Sendmail 升级到新的版本, 只需要把执行参数“-i”改为“-U”即可, 如下:

```
#rpm -Uvh sendmail-8.11.6-3.i386.rpm //更新主程序包
```

#### (2) Sendmail 主要文件

以 Red Hat 7.2 为例, Sendmail RPM 包是 Sendmail 的 8.11.6-3 的版本。解包之后, 主要的文件如表 3.11 所示。

表 3.11 Red Hat 7.0 中与 Sendmail 有关的文件(部分)

文件	说明
/etc/aliases	别名文本(文件)
/etc/aliases.db	别名文件(数据库)
/usr/bin/newaliases	用于从/etc/aliases 生成/etc/aliases.db
/etc/mail/access	邮件传送的处理规则设置文件(文本)
/etc/mail/access.db	邮件传送的处理规则设置文件(数据库)
/etc/rc.d/init.d/sendmail	启动脚本
/etc/sysconfig/sendmail	
/usr/sbin/sendmail	Sendmail 程序
/usr/share/man/	手册目录
/etc/sendmail.cf	Sendmail 的配置文件
/var/log/statistics	日志文件
/var/spool/mqueue	邮件队列文件

### (3) 配置/etc/sendmail.cf 文件

Sendmail 的配置文件是 sendmail.cf, 它包含了大部分的配置信息, 控制着 Sendmail 运行。sendmail.cf 也是一个文本文件, 它主要有三个重要的功能:

- 定义 Sendmail 的环境
- 按照接收邮件程序的语法重写地址
- 从地址映射出传输邮件所必需的指令

#### ① sendmail.cf 文件的结构

sendmail.cf 文件通常由一些节组成, 常见的节如表 3.12 所示。

表 3.12 sendmail.cf 文件中常见的节

节名	说明	是否修改
本地信息(Local info)	定义单个主机的专用信息	是
通用宏(General macros)	定义有关本地网络的专用信息	是
类(Class)	定义用于特殊邮件传输程序的主机名群或域名群	否
版本号(Version Number)	标识 sendmail.cf 文件的版本号	是
专用宏(Special Macros)	定义由 Sendmail 所用的特殊的宏	否
选项(Options)	定义 Sendmail 的各个选项	否
报文优先值(Message Precedence)	定义 Sendmail 使用的各种报文的优先级值	否
可信任用户(Trusted Users)	定义在发送邮件时不检查发送者地址的用户	一般不
报头格式(Format of Header)	定义 Sendmail 插入邮件的报头格式	否
重写规则(Rewriting Rules)	定义重写邮件地址时使用的规则	一般不
邮件程序(Mailer)	定义 Sendmail 调用邮件传输程序时所使用的指令	否
置零规则(Ruleset Zero)	定义一组称为“置零规则”的特殊重写规则	一般不

续表		
节名	说明	是否修改
置零规则中与及其有关的部分 (Machine-dependent Part of Rule- set Zero)	定义专用的置零规则部分，根据系统配置的邮件程序的不同而不同	一般不

② Sendmail 的配置命令概述

sendmail.cf 文件的语法很难懂，因为其命令和变量都只有一个字符，且单个字符的命令和一个字符的变量很容易造成混乱。

虽然这种语法非常难于理解，但是便于记忆，即每一行的第一个字符都是命令，根据这个字符就可以确定该命令是什么，从而也就可以确定它的结构。表 3.13 列出了 sendmail.cf 的语法和命令。

表 3.13 sendmail.cf 的配置命令

命令	命令语法	命令含义
定义宏(D)	Dxvalue	设置宏变量 x 的值为 value(单值)
定义类(C)	Ccword1[word2,...]	设置类变量 c 的值为 word1, word2, ...
装载类(F)	Fcfile	从文件 file 中装入类(使用一个文件内容定义类变量)
设置选项(O)	Oovalue	设置选项 O 的值为 value
可信用户(T)	Tuser1[user2],...	可信任用户是 user1, user2,...
设置优先级(P)	Pname=number	设置 name 的优先级为 number
定义邮件程序(M)	Mname, {field: value}	定义邮件程序 name
定义报头(H)	H[?mflag?]name: format	设置报头格式
设置规则集(S)	Sn	规则集 n 的开始
定义规则(R)	Rlhs rhs comment	将 lhs 格式改写为 rhs 格式

由于配置命令与它的变量或值之间没有空格，或用其他任何字符作间隔标志，因此使得这种“聚集在一起”的命令格式很难懂。例如：

```
DDxyz.com
```

这一行以字母 D 开始，也就是说这是一个宏定义命令。D 命令的变量应为宏的名字，由第二个字符指定，即定义了一个名为 D 的宏，宏 D 的值为 xyz.com。

③ sendmail.cf 文件的获得

由于 sendmail.cf 文件的配置极其复杂，所以没有人试图重新完整地编写一个 sendmail.cf 文件。在 Sendmail 的源代码分发中，为大多数的配置建立了模板文件。我们可以从模板文件中选择一个，再针对自己的需要做进一步修改。或者干脆用 Red Hat 7.0 中的 sendmail.cf 文件直接修改。

在提供的模板文件中，最常用的是 tcpproto.mc 文件，它直接用于与 TCP/IP 网络的连接。由于该模板文件是.mc 格式，所以需要下面的命令将其转换为.cf 格式：

```
#m4 tcpproto.mc >sendmail.cf
```



产生了 sendmail.cf 文件之后，用它覆盖/etc/目录下的 sendmail.cf 文件。

模板文件在结构上，一般遵从下列规则：

- 每台主机设置的“本地信息”通常位于文件的开头
- 相同的命令通常集中在一起
- 大部分文件都包含重写规则
- 文件的最后可能包含着邮件程序的定义，并且掺杂着个别邮件程序的重写规则。

重要的是应该认识到，对于一个典型的系统，sendmail.cf 文件有多少需要修改之处。如果选择了一个合适的样本文件，需要修改的内容则很少。从表 3.12 的第三列中的回答可以看到只需要修改和本地相关的一些信息。由此看来，Sendmail 的配置是一项很普通的任务。

这里就不罗列 Sendmail 的全部配置命令及其所有变量的意义，因为这实在是太多了，而且对于一个小型的局域网，只需按上面所说的，对模板文件稍加修改即可。

下面介绍一下常需要修改的部分：(这里域名为 abc.com.cn，邮件服务器的主机名为 mail，邮件服务器 IP 地址为 210.45.12.30 为例)

- 修改主机名

将行：

```
Cwlocalhost
```

修改为：

```
Cwmail.abc.com.cn abc.com.cn
```

这里主要是定义邮件地址形式，说明本地既可接收地址为 XXX@mail.abc.com.cn，也可接收 XXX@abc.com.cn 的邮件。

这里说明一点，这一行不作修改也可以，因为在这行后面有一条：

```
Fw/etc/mail/local-host-names
```

表明了 w 类可从/etc/mail/local-host-names 文件中读取，/etc/mail/local-host-names 文件需要用户手工创建，并在该文件中定义本机的拥有的域名信息，其内容为：

```
abc.com.cn  
mail.abc.com.cn
```

- 定义域名

将行：

```
DM
```

修改为：

```
DMabc.com.cn
```

#### (4) 配置/etc/mail/access 文件

/etc/mail/access 文件用于控制邮件传送的处理规则。下面是 Red Hat 7.0 中默认的/etc/mail/access 文件内容：

```
# Check the /usr/doc/sendmail-8.11.0/README.cf file for a description
# of the format of this file. (search for access_db in that file)
# The /usr/doc/sendmail-8.11.0/README.cf is part of the sendmail-doc
# package.
#
# by default we allow relaying from localhost...
localhost.localdomain      RELAY
localhost                  RELAY
127.0.0.1                  RELAY
```

/etc/mail/access 文件的格式为:

```
IpAddress|DomainName      RELAY|REJECT|OK|DISCARD
```

其中 RELAY 表示允许传送; REJECT 表示拒绝传送; OK 表示允许为拒绝域内的个别用户传送; DISCARD 表示丢弃。这种情况下, 邮件看上去是正常投递了, 但是由于没有人接收, 邮件会自动地“消失”在网络中。下面是一些例子:

```
202.99.11.120      RELAY      #允许为主机 202.99.11.120 传送
202.99.11          RELAY      #允许为网段 202.99.11 内的所有用户传送
abc.com.cn         RELAY      #允许为域 abc.com.cn 内的所有用户传送
xyz.com.cn         REJECT     #拒绝为域 xyz.com.cn 内的所有用户传送
abc.xyz.com.cn     OK         #但是允许为 abc.xyz.com.cn 传送
```

由于 Sendmail 并不直接读取/etc/access 文件, 而是读取由该文件创建的数据库(.db)文件, 因此在修改完该文件以后, 应该使用下面的命令, 使其生成相应的数据库文件:

```
#/usr/bin/makemap /etc/mail/access.db</etc/mail/access
```

在产生/etc/mail/access.db 文件后, 用户不需要重新启动, 所更改的设置值就会立即生效。此步骤也可以不做, 但需要重新启动 Sendmail, 因为 Sendmail 守护进程每次重新启动时都自动生成.db 文件。

#### (5) 配置/etc/aliases 文件

别名是 Sendmail 最重要的功能之一, 它的使用虽然简单, 但却能发挥强大的功能。Sendmail 的别名被定义在 aliases 文件中, 这个文件的位置是由 Sendmail 的配置文件 sendmail.cf 中的“O AliasFile=该文件的绝对路径”来指定的, 一般名字是/etc/aliases。Aliases 也是一个文本文件, 其中的每一行的格式如下:

```
alias: recipient [, recipient]
```

其中, alias 为邮件地址中的用户名, 而 recipient(收信人)是实际接收该邮件的用户。下面简单介绍定义别名有何作用:

##### ① 为单个用户指定别名

系统管理员可以为单个用户指定别名, 指定别名的目的主要有两个: 一是使用别名来保护合法用户的账号不被泄漏, 例如: 用户王蕾的登录账号设为 w457, 而该用户对外的电子邮件账号可以是 wanglei, 由于两个账号不同, 则需要在别名文件中添加如下的行:

```
wanglei:          w457
```

二是使用别名来将约定俗成的邮件转给一个真实的用户,例如,在 Web 页中一般指定管理员电子邮件为 `webmaster@abc.com.cn` 或 `administrator@abc.com.cn`,但 `webmaster` 和 `admininistrator` 往往在系统中不是一个真实用户,邮件系统必须要把它转给一个真正的系统管理员,如 `Jim@abc.com.cn`,则需要在别名文件中添加如下的两行:

```
webmaster:      jim
administrator:  jim
```

② 将发给特殊用户的邮件转发给实际用户。当系统守护进程(daemon)需要发信通知某个用户时,由于没有人能真正使用 `daemon` 的用户名登录,也就谈不上收信。因此,将邮件先发给假(pseudo)账号,然后在转发给实际用户,如 `root`。例如:

```
bin:            root
daemon:         root
adm:            root
lp:             root
sync:           root
shutdown:       root
halt:           root
mail:           root
news:           root
uucp:           root
```

### ③ 转发邮件

例如,主机 `mail.abc.com.cn` 上的用户 `Kate` 转到了另一家公司,其新账号是 `Kate@xyz.com.cn`,那么,原公司的系统管理员可在别名文件中加入:

```
Kate: Kate@xyz.com.cn
```

这样,发送到 `Kate@abc.com.cn` 的邮件会由主机 `mail.abc.com.cn` 自动转发到 `Kate@xyz.com.cn`。

### ④ 实现邮件列表

别名最重要的功能就是实现邮件列表。有了邮件列表,在发送 E-mail 时,只要填写一个接收者地址就可以同时向多个人发信。例如,在别名文件中添加:

```
net_group:      Osmond, Tom, Stillman, Patrcko
owner-net_group: Tom
```

那么,通过地址 `net_group@abc.com.cn` 就可以给网络组的全体成员 `Osmond`、`Tom`、`Stillman` 和 `Patrcko` 发信。第二行表示由 `Tom` 负责维护 `net_group` 这个邮件列表,若在传输信件给 `net_group` 时发生错误,就将有关的错误信息发送给 `Tom`。

由于 `Sendmail` 并不直接读取 `/etc/aliases` 文件,而是读取由该文件创建的数据库(.dbm)文件,所以当修改完 `/etc/aliases` 文件后,必须使用 `newaliases` 命令生成该数据库文件。

### (6) Sendmail 与域名系统的关系

电子邮件与域名系统的关系非常密切。在域名数据库中,有专门为电子邮件服务设置的 `MX` 记录。例如:

	IN	MX	10	mail
	IN	MX	20	mail1
mail	IN	A	202.99.11.120	
mail1	IN	A	202.99.11.121	

如果有一个 SMTP 客户要发送邮件给 XXX@abc.com.cn, 它将查询 abc.com.cn 域中有关 MX 记录, 得到了上述信息后, 它首先试图与具有较高邮件交换优先级(10)的主机 mail 发起 SMTP 连接, 如果连接成功, 就可以将信发送给 mail; 如果连接失败, 就试图与具有较低邮件交换优先级(20)的主机 mail1 发起 SMTP 连接, 如果连接成功, 就可以将信发送给 mail, 而 mail1 接收到这封信后, 就将其存放在邮件队列中, 每隔一段时间就尝试将此信发送给 mail。在这个过程中, 有关主机 mail 和 mail1 的 IP 地址将通过它们的 A 记录得到。必须注意, 为了避免无限循环发送, MX 记录是非递归的。

### (7) 运行 Sendmail

Sendmail 在系统中是一个守护进程(daemon), 监听端口号为 25。通常在开机时就已经自动启动了。也可使用下面的命令启动或重新启动 Sendmail 守护进程。启动命令是:

```
#/etc/rc.d/init.d/sendmail start
```

若对配置文件修改后, 使其生效, 可以重新启动 Sendmail 守护进程, 命令是:

```
#/etc/rc.d/init.d/sendmail restart
```

如果设定 Sendmail 服务在计算机启动时自动启动或不启动, 可以使用 ntsysv 命令将它加到引导程序中, 也可以通过 chkconfig 命令来设定, 该命令格式是:

```
chkconfig [--level <运行级>] <名字> [on|off]
```

例如, 我们希望计算机启动运行级别 3、5 时启动 Sendmail 服务, 则命令为:

```
#chkconfig --level 35 sendmail on
```

再如我们希望计算机启动运行级别 4 时不启动 Sendmail 服务, 则命令为:

```
#chkconfig --level 4 sendmail off
```

如果希望在任务运行级别下都启动或不启动 Sendmail 服务, 只需不设定 “[--level <运行级>]” 就可以了, 即:

```
#chkconfig sendmail on
#chkconfig sendmail off
```

### (8) 测试 Sendmail 服务

启动 Sendmail 之后, 接下来测试 Sendmail 是否能正常工作。由于 Sendmail 默认的通信端口为 25, 所以可以利用 telnet 命令登录到第 25 号端口, 测试 Sendmail 是否已经启动:

```
#telnet localhost 25
```

如果用户可以看到登录信息, 则表示 Sendmail 已经启动了。

## 2. 电子邮件阅读服务器 POP3 和 IMAP 的安装和配置



如果已经正确地安装了 Sendmail 服务器, 用户就可以登录到邮件主机进行读或写邮件了。但现在 Windows 用户都习惯于使用如 Outlook Express 这样的电子邮件客户端软件来接收和发送邮件, 这就需要在邮件主机中增加电子邮件阅读服务器。电子邮件阅读服务器主要有两种, 一种是 POP3(POP, Post Office Protocol, 即邮局协议, 3 表示第 3 版)服务器, 另一种是 IMAP(Internet Message Access Protocol, 因特网报文存取协议)服务器。

#### (1) 安装 POP3 和 IMAP 服务器

如果用户在安装 Linux 时已经安装了 POP3 和 IMAP 服务器程序 ipop3d 和 imapd, 就不需要另行安装。但如果不确定已经安装了 ipop3d 和 imapd, 则可执行以下命令确认:

```
#rpm -qa |grep imap
imap-2000c-15    //若出现此行, 则表示已经安装了 pop3 和 imap 服务器
```

如果用户发现系统未安装 pop3 或 imap 服务器软件, 则可以在网上下载相应的安装包, 也可以在 Red Hat Linux 安装盘中找到这两种服务器的安装包。然后执行以下命令:

```
#rpm -ivh imap-2000c-15.i386.rpm    //安装 imap 软件包
```

如果从旧版本升级至新版本, 则只需要把执行参数“-i”改为“-U”即可:

```
#rpm -ivh imap-2000c-15.i386.rpm    //安装 imap 软件包
```

这里需要说明一点, 由于 Red Hat Linux 将 POP3 和 IMAP 程序编成了一个 imap 组件, 因此只需安装这个组件即可。安装完成之后, 在/usr/sbin/目录中就可以找到 imapd、ipop2d 和 ipop3d 这 3 个文件, 每个文件的文件名都以“d”结尾表示 daemon(守护程序)。

#### (2) 设置和启动 POP3 和 IMAP 服务器

安装好 POP3 和 IMAP 服务器之后, 接着就需要修改配置文件。

##### ① 修改/etc/services

需要确定/etc/services 文件有以下几行内容, 同时这些内容未被加上注释符“#”:

pop2	109/tcp	pop-2	postoffice
pop2	109/udp	pop-2	
pop3	110/tcp	pop-3	
pop3	110/udp	pop-3	
imap	143/tcp	imap2	
imap	143/udp	imap2	

##### ② 修改/etc/xinetd.d/ipop3 和/etc/xinetd.d/imap 文件

如果要启动 pop3 服务, 则需要修改/etc/xinetd.d/ipop3, 把 disable 的值 yes 改成 no。这个文件内容大致如下:

```
service pop3
{
    disable = no                //将 yes 改为 no, 表示启动该服务
    socket_type = stream
    wait = no
    user = root
    server = /usr/sbin/ipop3d
```

```

        log_on_success  += HOST DURATION
        log_on_failure  += HOST
    }

```

以同样的方法修改/etc/xinetd.d/imap 文件, 启动 imap 服务。

### ③ 重新启动 xinetd

要想修改内容立即生效, 可以重新启动 xinetd 程序, 命令是:

```
#/etc/rc.d/init.d/xinetd restart
```

### (3) 测试 POP3 和 IMAP 服务器

和测试 Sendmail 服务器一样, 可以通过 telnet 命令分别登录到 110 端口来测试 POP3 服务, 登录到 143 端口来测试 IMAP 服务。其命令分别是:

```

#telnet localhost 110          //测试 POP3 服务器
#telnet localhost 143          //测试 IMAP 服务器

```

如果登录成功, 则表明该服务器已成功安装并启动。

## 3.3.2 典型例题分析

**例** 阅读以下说明, 回答问题 1~5, 将答案填入对应的答案栏内。

### 【说明】

在 Linux 下安装配置 Sendmail 服务, Sendmail 服务程序需要读取一些配置文件, 以下列出了 Sendmail 的三个配置文件的主要内容。

- /etc/mail/local-host-names 文件内容:

```

xyz.com.cn
mail.xyz.com.cn

```

- /etc/mail/access 文件内容:

```

localhost.localdomain    RELAY
localhost                 RELAY
127.0.0.1                 RELAY
210.45.12                 RELAY
xyz.com.cn                RELAY
210.45.13                 REJECT
abc.com.cn                REJECT

```

- /etc/aliases 文件内容:

```

bin:           root
daemon:        root
adm:           root
lp:            root
sync:          root
shutdown:      root
halt:          root

```

```
mail:          root
news:          root
uucp:          root
webmaster:     tom
jack:          jack@sohu.com.cn
net_group:     Osmond, Tom, Stillman, Patcrko
owner-net_group: Tom
```

【问题1】该电子邮件服务器将接收电子邮件地址格式是什么样的电子邮件？用户名使用 XXXX 代替，写出完整格式(假设 DNS 已做解析)。

【问题2】该电子邮件服务器将允许传送哪个网络和哪个域的电子邮件？该电子邮件服务器将拒绝传送哪个网络和哪个域的电子邮件？

【问题3】该电子邮件服务器收到一封寄给 webmaster@xyz.com.cn 的邮件时，作何处理？该电子邮件服务器收到一封寄给 net\_group@xyz.com.cn 的邮件时，又作何处理？

【问题4】命令 `#/usr/bin/makemap /etc/mail/access.db</etc/mail/access` 的作用是什么？

【问题5】当对 Sendmail 的配置文件作修改后，怎样使配置文件立即生效(不重新启动计算机)？

分析：该题主要考查考生对 Linux 下 Sendmail 服务配置的掌握情况。

在 Linux 下 Sendmail 服务器的配置文件主要有以下几个：主配置文件 `sendmail.cf`、邮件传送控制文件 `access` 和别名文件 `aliases`。但主配置文件 `sendmail.cf` 配置起来非常复杂，在一般应用中，该文件可以使用系统模板来生成，只需做很少的修改。主要是修改主机名和域名等内容。为了减少修改，在 `sendmail.cf` 中有一行：

```
Fw/etc/mail/local-host-names
```

该行用于从 `/etc/mail/local-host-names` 读取本地主机名，这样用户只需把主机名配置放置在 `/etc/mail/local-host-names` 中，从而减少了对 `sendmail.cf` 的修改。

问题1：文件 `/etc/mail/local-host-names` 主要是用定义本机拥有的域名信息，决定了本机可以接发什么样后缀(电子邮件地址@后的内容)的电子邮件。本例中，该文件有两行，那么该邮件服务器可接收形式为 `XXXX@xyz.com.cn`、`XXXX@mail.xyz.com.cn` 的电子邮件。

问题2：`/etc/mail/access` 文件用来控制邮件传送的处理规则，即允许传送哪个主机、网络和域名的电子邮件(RELAY)，拒绝传送哪个主机、网络和域名的电子邮件(REJECT)，丢弃哪个主机、网络和域名发来的电子邮件(DISCARD)。本例中，将允许网络 `210.45.12.0/24` 和域 `xyz.com.cn` 内所有用户的电子邮件的传送，将拒绝网络 `210.45.13.0/24` 和域 `abc.com.cn` 内所有用户的电子邮件的传送。

问题3：别名文件 `aliases` 是 Sendmail 另外一个重要的配置文件，它定义了邮件地址中的用户名和实际接收该邮件的用户的映射，以实现保护用户账号、邮件转发和邮件列表等功能。在本例中，该电子邮件服务器收到一封寄给 `webmaster@xyz.com.cn` 的邮件时，将邮件传输给用户名为 Tom 的用户；当电子邮件服务器收到一封寄给 `net_group@xyz.com.cn` 的邮件时，将邮件传输给用户名为 Osmond、Tom、Stillman、Patcrko 的用户各一份，从而实现了邮件列表功能。

问题4：Sendmail 不能直接读取邮件传送控制配置文件 `access`，只能读取其相应的数据

库文件,因此在修改完该 access 文件以后,应该用一条命令为其生成相应的数据库文件。而这条命令就是:

```
#/usr/bin/makemap /etc/mail/access.db</etc/mail/access
```

问题 5: 在 Sendmail 服务器,若对配置文件修改后不能立即生效,要使其立即生效,必须重新启动 Sendmail 守护进程,命令是:

```
#/etc/rc.d/init.d/sendmail restart
```

答案:

【问题 1】XXXX@xyz.com.cn、XXXX@mail.xyz.com.cn。

【问题 2】允许网络 210.45.12.0/24 和域 xyz.com.cn 内所有用户的电子邮件的传送,拒绝网络 210.45.13.0/24 和域 abc.com.cn 内所有用户的电子邮件的传送。

【问题 3】该电子邮件服务器收到一封寄给 webmaster@xyz.com.cn 的邮件时,将邮件传输给用户名为 Tom 的用户;当电子邮件服务器收到一封寄给 net\_group @xyz.com.cn 的邮件时,将邮件传输给用户名为 Osmond、Tom、Stillman、Patrcko 的用户各一份。

【问题 4】创建传送控制配置文件 access 相应的数据库文件。

【问题 5】#/etc/rc.d/init.d/sendmail restart。

### 3.3.3 同步练习

阅读以下说明,回答问题 1~5,将答案填入对应的答案栏内。

【说明】

某公司使用了一台安装有 Linux 操作系统的 PC 服务器作为电子邮件服务器,邮件发送服务使用 sendmail 8.0,下面是 Sendmail 的三个配置文件的内容片断。

● /etc/sendmail.cf 文件片断:

```
Cwmail.aapla.edu.cn aapla.edu.cn
#Fw/etc/mail/local-host-names
DMAapla.edu.cn
```

● /etc/mail/access 文件内容:

```
localhost.localdomain      RELAY
localhost                  RELAY
127.0.0.1                  RELAY
(1)
aapla.edu.cn               RELAY
(2)
```

● /etc/aliases 文件内容:

```
bin:      root
daemon:   root
adm:      root
lp:       root
```



```

sync:                root
shutdown:            root
halt:                root
mail:                root
news:                root
uucp:                root
administrator:       ketty
                    (3)
net_group:            Osmond, Tom, Stillman, Patcrko
owner-net_group:     Tom

```

【问题 1】该电子邮件服务器将接收电子邮件地址格式是什么？用户名使用 XXXX 代替，写出完整格式。(假设 DNS 已做解析)

【问题 2】假设该公司的用户都在 220.96.73.0/24 这个 C 类网络上收发电子邮件，则(1)处该填写什么内容？

【问题 3】在使用过程中，发现域 abc.com.tw 上有人使用该服务器发送电子邮件，为了实现拒绝，在(2)处该填写什么内容？

【问题 4】该公司有一名员工辞职了，他原先在这台服务器有一个账号 Jim，现在的他在 tom.com 中申请了一个免费邮箱，地址为 jim998@tom.com。若想把发给 Jim 邮件的转发到他的新邮箱中，则(3)处该填写什么内容？

【问题 5】命令 #/usr/bin/newaliases 的作用是什么？

【问题 6】如何测试 sendmail 服务器已成功启动？

### 3.3.4 同步练习参考答案

【问题 1】XXXX@mail.aapla.edu.cn、XXXX@aapla.edu.cn。

【问题 2】220 96.73          RELAY

【问题 3】abc.com.tw        REJECT

【问题 4】Jim: jim998@tom.com

【问题 5】创建别名配置文件/etc/aliases 对应的数据库(.db)文件 aliases.db。

【问题 6】telnet localhost 25

## 3.4 FTP 服务器

### 3.4.1 考点辅导

#### 3.4.1.1 Windows Server 2003 的 IIS 下 FTP 服务器的安装与配置

##### 1. FTP 服务器的安装

Windows Server 2003 中 IIS 里内置了 FTP 服务模块，安装比较简单。由于 FTP 不是默

认的安装组件,系统不会自动安装,因此必须采用 Windows 组件方式来安装 FTP 服务。具体操作步骤如下:

(1) 单击【开始】|【设置】|【控制面板】,在控制面板中,双击【添加/删除程序】图标,选择【添加/删除 Windows 组件】。

(2) 在【Windows 组件向导】对话框的列表框中选择【应用程序服务器】,如图 3.47 所示。

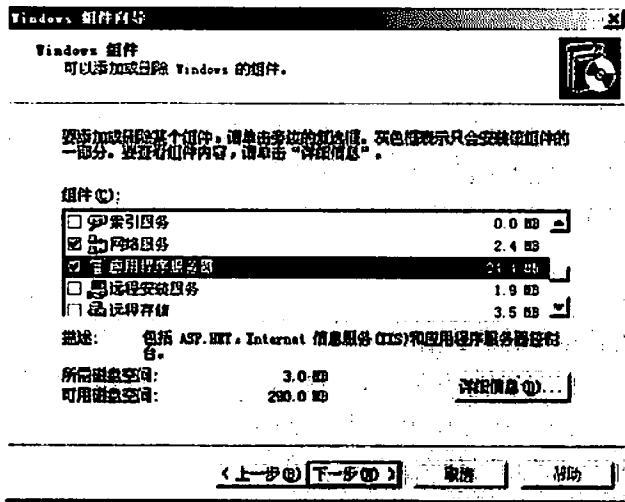


图 3.47 【Windows 组件向导】对话框

(3) 单击【详细信息】按钮,弹出【应用程序服务器】对话框,选中【Internet 信息服务(IIS)】复选框,如图 3.48 所示。

(4) 在【应用程序服务器】对话框中单击【详细信息】按钮,系统显示【Internet 信息服务(IIS)】对话框,选中【文件传输协议(FTP)服务】复选框,单击【确定】按钮,按提示信息插入光盘,系统自动完成 FTP 服务的安装,如图 3.49 所示。

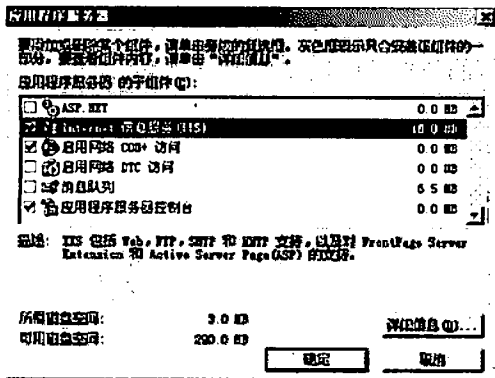


图 3.48 【应用程序服务器】对话框

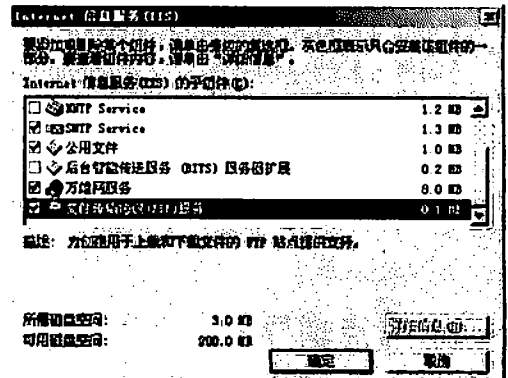


图 3.49 【Internet 信息服务(IIS)】对话框

## 2. FTP 服务器的配置

FTP 服务器的“默认 FTP 站点”所在主目录为 C:\inetpub\ftproot(若系统安装在 D 盘,

则为 D:\inetpub\ftproot), IP 地址为“全部未分配”, 允许来自任何 IP 地址的用户以匿名方式访问。只需要将共享文件复制到 C:\inetpub\ftproot 目录下, FTP 客户端用户就可以匿名登录进行文件下载, 但由于默认情况下主目录为只读方式, 所以客户端只能下载而不能上传。为了更好地管理 FTP 服务器, 需要对它进行适当的配置, 方式如下。

(1) 修改 IP 地址和端口

① 依次单击【开始】|【管理工具】|【Internet 信息服务(IIS)管理器】, 打开 IIS 控制台, 显示 IIS 信息, 包括 FTP 站点、应用程序池、网站以及 Web 服务扩展等, 如图 3.50 情所示。

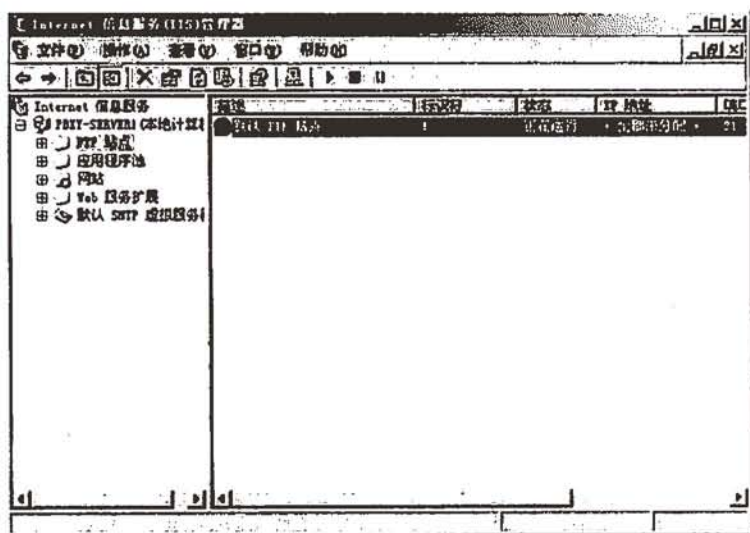


图 3.50 IIS 控制台

② 展开窗口左边的【FTP 站点】控制树, 选中【默认 FTP 站点】, 单击工具条上的按钮可以实现对 FTP 站点的启动、暂停、停止等操作。

③ 右击相应站点, 在弹出的快捷菜单中选择【属性】子菜单, 系统将显示 FTP 站点属性信息, 如图 3.51 所示。其中【FTP 站点】选项卡包括 FTP 站点的标识, FTP 站点连接和日志记录信息, 其中 IP 地址和端口号在 FTP 站点标识中设置。

【描述】作为 FTP 服务器的名称显示在“Internet 信息服务”窗口的目录中, 如果在一台计算机中安装了多个 FTP 服务器, 管理员可根据“标识”对各台 FTP 服务器加以区分。

【IP 地址】下拉列表框用于设置该 FTP 站点的 IP 地址。Windows Server 2003 操作系统中允许安装有多块网卡, 而且每块网卡也可以绑定多个 IP 地址, 通过设置【IP 地址】文本框中的信息, FTP 客户端利用设置的这个 IP 地址来访问该 FTP 服务器。通过下拉列表框从一个或多个地址中选择一个作为“IP 地址”。

【TCP 端口】是指用户与 FTP 服务器进行连接并访问的端口号, 默认的端口号为 21。服务器也可设置一个任意的 TCP 端口号, 若更改了 TCP 端口号, 客户端在访问时需要在 URL 之后加上这个端口号, 因此必须让客户端事先知道, 否则就无法进行 TCP 连接。

比如可以设置标识为 MP3, IP 地址为 192.168.0.61, 端口号为 21, 如图 3.52 所示。

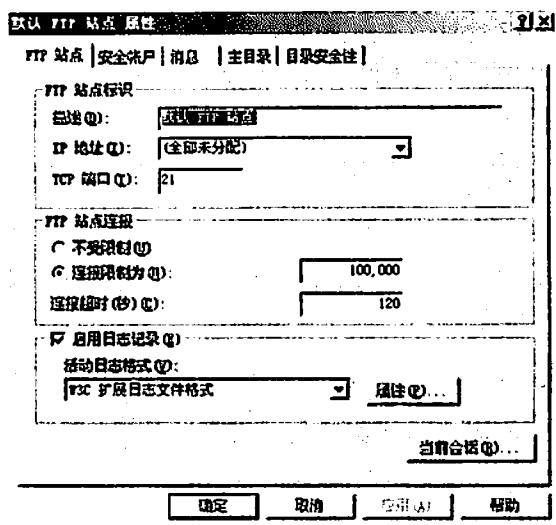


图 3.51 FTP 站点属性设置

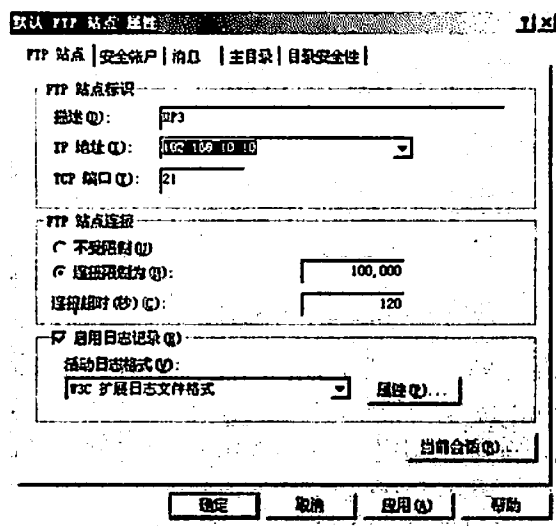


图 3.52 配置后的 FTP 站点属性

## (2) 限制连接数量

在【FTP 站点】选项卡的【FTP 站点连接】中有以下 3 个选项。

- ① 【不受限制】：该选项允许同时发生的连接数将不受任何限制。
- ② 【连接限制】：该选项限制允许同时发生的连接数为某一特定值，这一特定值由用户在文本框中输入。
- ③ 【连接超时】：当连接超时达到某一时间，服务器就自动断开该连接。

由于服务器配置、性能等的差别，有些服务器不能满足大访问量的需要，往往造成超时甚至死机，因此需要设置连接限制。同时，为了确保 FTP 协议在连接失败时关闭连接，因此需要设置连接超时。

## (3) 设置主目录



主目录信息在属性信息的【主目录】选项卡中设置。所谓主目录是指映射为FTP根目录的文件夹，FTP站点中的所有文件将保存在该目录中。系统默认的FTP主目录为C:\inetpub\ftproot(其中，C为操作系统安装的逻辑盘符，若系统安装在D盘，则为D)，可以根据用户的需要更改主目录和其属性。

可以把主目录修改为计算机中的其他文件夹，甚至可以是另一台计算机上的共享文件夹。同时，管理者可以修改用户对站点的访问权限，以及目录的列表风格，如图3.53所示。

#### (4) 访问安全设置

FTP站点的安全非常重要，Windows Server 2003中对FTP服务器可配置用户身份认证、限制访问FTP的IP地址，从而确保站点的安全。

① 禁止匿名访问。禁止匿名访问在属性信息的【安全账户】选项卡中设置。在默认情况下，FTP站点允许用户匿名访问，如果站点安全性要求较高，取消【允许匿名连接】的选择即可禁止用户匿名访问该FTP站点，如图3.54所示。

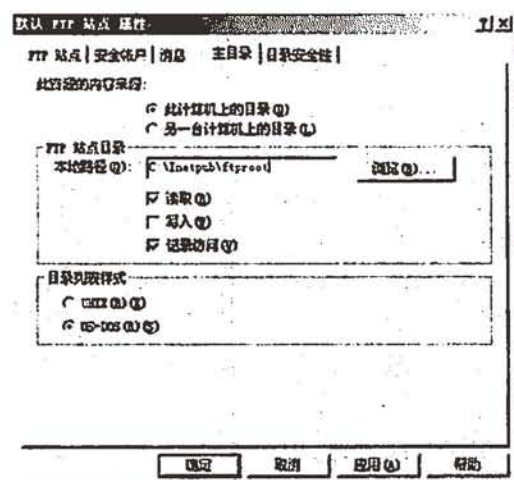


图 3.53 【主目录】选项卡

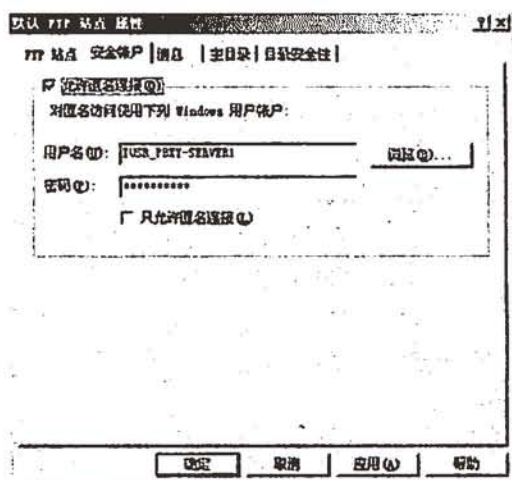


图 3.54 【安全账户】选项卡

② 限制IP地址。限制IP地址在FTP站点属性的【目录安全性】选项卡中设置。通过对IP地址的限制可以只允许某些特定的计算机访问该站点，从而避免外界恶意攻击，如图3.55所示。有两种方式来限制IP地址的访问，一是【授权访问】，其含义是除列表中IP地址的主机不能访问外，其他所有主机都可以访问该FTP站点，主要是用于给FTP服务器加入“黑名单”；二是【拒绝访问】，其含义是除列表中IP地址的主机能访问外，其他所有主机都不能访问该FTP站点，主要用于内部FTP，以防止外部主机访问该FTP站点。

#### (5) 设置消息

消息主要是指在用户登录或退出时显示的信息。可在FTP站点属性的【目录安全性】选项卡中设置，如图3.56所示。在【欢迎】处填写用户登录时显示的信息，在【退出】处填写用户退出时显示的信息。在此选项卡中可以设置当超过最大连接人数时，给提出连接请求的客户机发送一条报错信息，若要设置此功能就在【最大连接数】处填写报错信息。

#### (6) 建立虚拟目录

当有个目录需要通过FTP站点进行发布，而又不是存放在主目录之下的目录时，称此

目录为 FTP 虚拟目录。

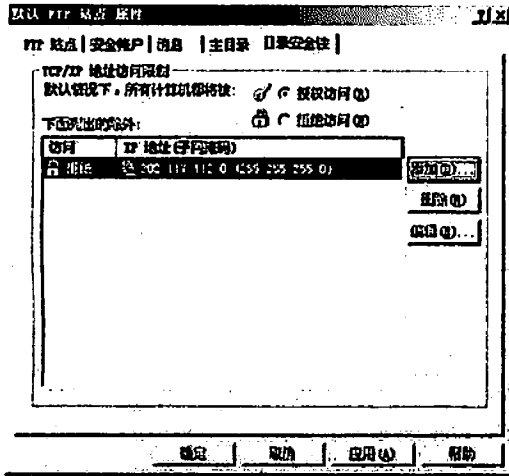


图 3.55 【目录安全】选项卡

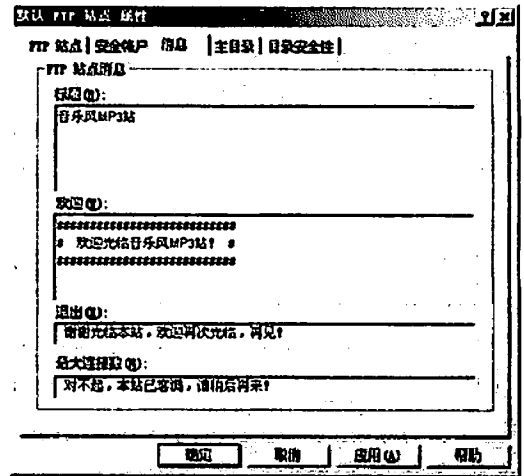


图 3.56 【消息】选项卡

建立虚拟目录的步骤如下：

① 右击 FTP 站点，在弹出的快捷菜单中选择【新建】|【虚拟目录】命令，打开【虚拟目录创建向导】。

② 在【虚拟目录别名】对话框中，输入虚拟目录别名(即访问时用的名字)，单击【下一步】按钮，如图 3.57 所示。

③ 在【FTP 站点内容目录】对话框中，输入虚拟目录所映射的真实路径，单击【下一步】按钮，如图 3.58 所示。

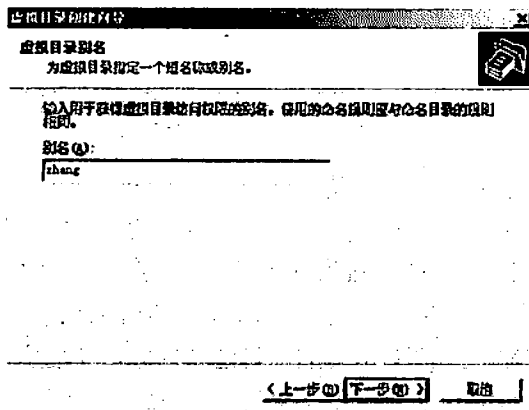


图 3.57 【虚拟目录别名】对话框

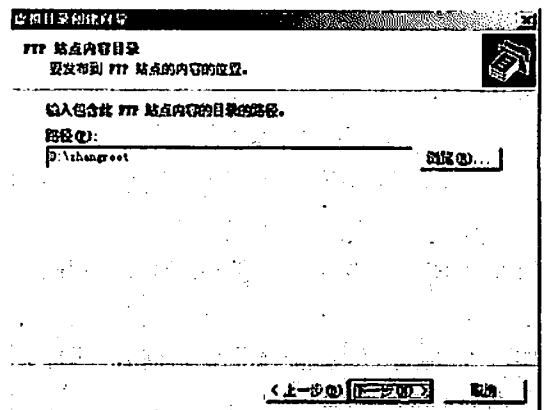


图 3.58 【FTP 站点内容目录】对话框

④ 在【访问权限】对话框中，设置该目录的访问权限，可为只读，也可以是写入。单击【下一步】按钮就完成了虚拟目录的建立，如图 3.59 所示。

虚拟目录和真实目录一样，也可以为其设置安全性和访问控制，默认情况都继承站点的安全性和访问控制，用户可自行修改，修改方法同上。

这里要注意一点，当一个注册用户登录到 FTP 站点时，若有和该用户账号同名的真实目录和虚拟目录时，将自动进入该目录。

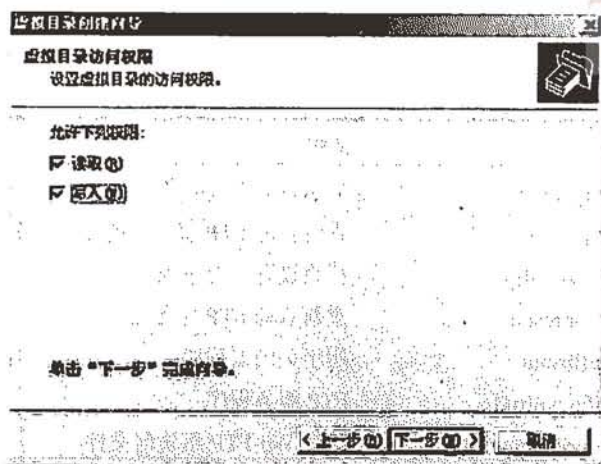


图 3.59 【虚拟目录访问权限】对话框

### 3.4.1.2 Linux 下 Wu-FTP 服务器的安装与配置

在 Linux 环境下使用的 FTP 服务器软件主要有 Wu-FTP、NcFTP 和 ProFTP 三种。由于 Wu-FTP 是目前最流行的一种免费 FTP 服务器软件，所以下面主要介绍 Wu-FTP。

#### 1. Wu-FTP 功能和特征

Wu-FTP 的特征：

- Wu-FTP 是基于 GPL 协议开发的，它是一个源码公开的自由软件；
- Wu-FTP 是历史最久的非商业 FTP 服务器程序之一，它的影响非常广泛；
- Wu-FTP 项目仍然继续进行，新的特性不断被加入；
- Wu-FTP 支持广泛的 UNIX 和类 UNIX 平台。

Wu-FTP 的功能：

- 可以控制不同网络和域的用户对 FTP 服务器的存取权限和访问时段；
- 使用者在下载文件时，可以自动对其进行压缩和解压缩工作；
- 可以记录文件上传和下载的全过程；
- 可以显示传输时的相关信息，方便用户及时了解目前的传输动态；
- 可以设置最大连接数，从而提高了效率，且有效地控制了负载；
- 可以暂时关闭 FTP 服务器，以便系统维护。

#### 2. Wu-FTP 服务器的获取与安装

Wu-FTP 有 RPM 包分发版本，可以从 Red Hat 网站下载或在 Red Hat 7.0 的光盘中找到。二进制的分发版本可以从 <ftp://ftp.wu-ftp.org/pub/wuftp> 处进行下载。

下面以 RPM 的安装为例介绍 Wu-FTP 的安装过程。

若在安装 Red Hat 时没有安装 Wu-FTP，则可以使用下面的命令进行安装：

```
#rpm -ivh wu-ftp-2.6.0.i386.rpm
```

若获得了更新版本的 Wu-FTP 的 RPM，可以使用下面的命令进行升级：

```
#rpm -Uvh wu-ftp-2.6.x.i386.rpm
```

当安装完成后，系统中将存在如表 3.14 所示的文件。

表 3.14 Wu-FTP 的主要文件

类型	文件名	说明
可执行文件	/usr/bin/ftpcount	显示目前在线人数
	/usr/bin/ftpwho	查看目前 FTP 服务器的连接情况
	/usr/sbin/ckconfig	检查设置是否正确
	/usr/sbin/ftprestart	重新启动 FTP 服务器
	/usr/sbin/ftpshut	用于关闭器程序
	/usr/sbin/in.wuftpd	FTP 服务程序
	/usr/sbin/privatepw	改变 Wu-FTP 组访问文件
配置文件	/etc/ftpaccess	Wu-FTP 的主配置文件，控制存取权限
	/etc/ftpconversions	用来控制当传输文件的时候是否进行压缩
	/etc/ftpusers	禁止某些用户登录
	/etc/ftphosts	禁止某些来自指定机器上的登录
	/etc/ftpgroups	创建用户组，这个组中的成员预先定义可以访问 FTP 服务器
手册	/usr/share/doc/wu-ftp-2.6.1/	存放 Wu-FTP 文档
文档	/usr/share/man/	存放 Wu-FTP 手册页

### 3. 启动 Wu-FTP

#### (1) 修改/etc/services

需要确定/etc/services 文件有以下一行内容，同时该内容未被加上注释符“#”：

```
ftp          21/ftp          ftp
```

#### (2) 创建/etc/xinetd.d/wu-ftp 文件，文件大致内容如下：

```
service ftp
{
    disable                = no
    socket_type             = stream
    wait                   = no
    user                   = root
    server                 = /usr/sbin/in.ftpd
    server_args             = -l -a
    log_on_success          += DURATION USERID
    log_on_failure         += USERID
    nice                   = 10
}
```

#### (3) 重新启动 xinetd

要想修改内容立即生效，可以重新启动 xinetd 程序，其命令是：



```
#/etc/rc.d/init.d/xinetd restart
```

#### (4) 测试 Wu-FTP 是否启动

和测试 Sendmail 服务器一样,可以通过 telnet 命令登录到 21 端口来测试 Wu-FTP 服务是否启动。其命令是:

```
#telnet localhost 21
```

如果登录成功,则表明该服务器已成功安装并启动。

### 4. Wu-FTP 服务器配置

#### (1) /etc/ftpuser 的配置

/etc/ftpuser 用来指定某些用户不能登录本 FTP 服务器。其实这个设置是十分简单的,只需要将要禁止的用户账号写入文件/etc/ftpuser 中。由于从系统的安全考虑,一般我们是不希望权限过大的用户和一些与命令名相同的用户进入 FTP 服务器。所以在默认的配置中,一般来说以下用户已经被列入了“黑名单”。

```
root
uucp
news
bin
adm
nobody
lp
sync
shutdown
halt
mail
```

#### (2) /etc/ftphosts 的配置

/etc/ftphosts 用来指定某些主机不能连接本 FTP 服务器。要禁止某些来自指定机器上的登录可以有两种方法,一种方法就是在/etc/ftpaccess 中设置 deny 命令,另一种更加简单的方法就是在/etc/ftphosts 中写入要禁止的主机的 IP 地址或域名。下面是一个/etc/ftphosts 文件的范例:

```
allow xyz *.abc.com.cn 210.102.0.0/16
deny tom *.hanker.com 131.222.154.0/24
```

例中允许用户 xyz 从域名以 abc.com.cn 为后缀的主机及 210.102.0.0/255.255.0.0 的主机上登录;禁止用户 Tom 从域名 hanker.com 为后缀的主机及 131.222.154.0/255.255.255.0 的主机上登录。当用户名为 anonymous 或 ftp 时,均表示匿名用户。

#### (3) /etc/ftpconversions 的配置

/etc/ftpconversions 文件主要定义用户从 FTP 服务器中下载文件时对文件进行格式转换的规则。例如压缩、解压缩、打包和开包等操作,这样用户就不必为.tar.gz、.tgz、.Z、.z 之类的文件伤脑筋了。

/etc/ftpconversions 文件的格式乍看上去很复杂,不过不必担心,基本上不用修改、设

置。下面是一个/etc/ftpconversions 文件, 它已经能够满足一般的使用需要了。

```
:.Z: : :/bin/compress -d -c %s:T_REG|T_ASCII:O_UNCOMPRESS:UNCOMPRESS
: : :.Z:/bin/compress -c %s:T_REG:O_COMPRESS:COMPRESS
.gz: : :/bin/gzip -cd %s:T_REG|T_ASCII:O_UNCOMPRESS:GUNZIP
: : :.gz:/bin/gzip -9 -c %s:T_REG:O_COMPRESS:GZIP
: : :.tar:/bin/tar -c -f - %s:T_REG|T_DIR:O_TAR:TAR
: : :.tar.Z:/bin/tar -c -Z -f - %s:T_REG|T_DIR:O_COMPRESS|O_TAR:TAR+COMPRESS
: : :.tar.gz:/bin/tar -c -z -f - %s:T_REG|T_DIR:O_COMPRESS|O_TAR:TAR+GZIP
```

如果想让 FTP 服务器有自动压缩、解压缩的功能, 必须先将一些压缩、解压缩的命令文件如 tar、gzip、gunzip、compress、uncompress 等命令文件复制到/home/ftpd/bin 目录下。

#### (4) /etc/ftppaccess 的配置

/etc/ftppaccess 是 FTP 服务器上最重要的配置文件, 它主要控制 FTP 存取权限, 直接关系到 FTP 服务器能否正常工作, 还有其他许多权限上的设置。下面是一个典型的配置实例。

```
loginfails 3
class local real *
class remote anonymous guest *
limit remote 100 Any /etc/ftpd/toomany.msg
message /etc/ftpd/welcome.msg login
compress yes local remote
tar yes local remote
private yes
passwd-check rfc822 warn
log commands real
log transfer anonymous guest inbound outbound
log transfer real inbound
shutdown /etc/ftpd/shut.msg
delete no anonymous,guest
overwrite no anonymous,guest
rename no anonymous
chmod no anonymous,guest
umask no anonymous
upload /home/ftpd * no
upload /home/ftpd /bin no
upload /home/ftpd /etc no
upload /home/ftpd /pub yes real 0644 dirs
upload /home/ftpd /incoming yes real guest anonymous 0644 dirs
alias in /incoming
email guest@xxx.net
email guest@yyy.net
deny *.com.tw /etc/ftpd/deny.msg
```

下面逐条进行讲解, 并给出每条设置的含义, 以便读者触类旁通, 根据自己 FTP 服务器的具体情况进行合理设置。

#### ● 登录重试次数

格式: loginfails [次数]

功能: 设置当用户登录到 FTP 服务器时, 允许用户输入错密码的次数。

实例: “loginfails 3”: 密码输入错误 3 次就切断连接。

- 定义用户类别

格式: class [类名] [real/guest/anonymous] [IP 地址]

功能: 这个指令用于设置 FTP 服务器上用户的类别。并可对客户端的 IP 地址进行限制, 允许某部分的 IP 地址或全部的 IP 地址访问。而在 FTP 服务器上的用户基本上可以分为以下 3 类:

- ① real 在该 FTP 服务器有合法账号的用户
- ② guest 有记录的匿名用户
- ③ anonymous 权限最低的匿名用户

实例: class local real \*: 定义一个名为 local 的类, 它包括在任何地方登录(\*代表所有 IP 地址)的 real 用户。

class remote anonymous guest \*: 定义一个名为 remote 的类, 它包括在任何地方登录的 anonymous 用户和 guest 用户。

- 登录人数的限制

格式: limit [类别] [人数] [时间] [文件名]

功能: 这个指令的功能是设置指定时间内指定的类别允许连接的人数上限。当达到人数上限的时候, 显示指定文件的内容。

实例: limit remote 100 Any/etc/ftpd/toomany.msg: 在任何时间内, remote 类的访问用户达到 100 人时, 将不再允许或无法产生新的连接。当第 101 位客户要连接时, 连接将失败, 并向用户出示文件/etc/ftpd/toomany.msg 的内容。

- 用户登录时显示的文件

格式: message [文件名称] [指令]

功能: 当用户执行指定的指令时, 系统将指定的文件内容显示出来。

实例: message/etc/ftpd/welcome.msg login: 当用户执行 login 命令时, 也就是登录到 FTP 服务器上的时候, 系统将显示文件/etc/ftpd/welcome.msg 的内容。

- 压缩功能

格式: compress [yes/no] [类别]

功能: 设置某个类别的用户可以使用 compress(压缩)功能。

实例: compress yes local remote: 允许 local 和 remote 两类用户都能使用 compress(压缩)功能。

- 归档功能

格式: tar [yes/no] [类别]

功能: 设置某个类别的用户可以使用 tar(归档)功能。

实例: tar yes local remote: 允许 local 和 remote 两类用户都能使用 tar 功能。

- 是否支持群组

格式: private [yes/no]

功能: 设置是否支持群组对文件的取用。

实例: private yes: 支持群组对文件的取用。

- 匿名用户密码检查

格式: passwd-check [none/trivial/rfc822] [enforce/warn]

功能: 设置匿名用户 anonymous 的密码使用方式。

none 表示不做密码验证, 任何密码都可以登录;

trivial 表示只要输入的密码中含有字符 “@” 就可以登录;

rfc822 表示密码一定要符合 RFC822 中所规定的 E-Mail 地址才能登录;

enforce 表示输入的密码不符合以上指定的格式就不允许登录;

warn 表示密码不符合规定时只出现警告信息, 仍然能够登录。

实例: passwd-check rfc822 warn: 希望能够得到符合规定的 E-Mail 作为密码, 但如果不是, 也允许登录。

- 操作日志

格式: log command [real/guest/anonymous]

功能: 设置某些用户登录后的操作记录在文件 /usr/adm/xferlog 中。

实例: log command real: 当 real 用户登录后, 将其操作记录下来。由于其他用户权限较低, 所以操作不会引起太大的安全隐患, 所以一般只需记下 real 用户的操作就可以了。

- 文件传送日志

格式: log transfer [real/guest/anonymous] [inbound/outbound]

功能: 设置某些用户的上载(inbound)和下载(outbound)操作日志。

实例: log transfer anonymous guest inbound outbound: 对于匿名用户要更加关注它们的文件操作, 所以无论上载、下载都进行记录。

log transfer real inbound: 对于合法用户则只记录他的上载记录。

- FTP 服务器关闭设置文件

格式: shutdown [文件名]

功能: FTP 服务器关闭的时间可以设置在后面所指定的文件中, 当设置的时间一到, 便无法登录 FTP 服务器了, 要恢复的话只有将这个文件删掉。而这个文件必须由指令 /bin/ftpsht 来生成。

实例: shutdown /etc/ftpd/shut.msg

- 删除文件权限设置

格式: delete [yes/no] [real/anonymous/guest]

功能: 设置是否允许指定用户使用 delete 命令删除文件。默认是允许。

实例: delete no anonymous,guest: 为了更好地管理 FTP 服务器, 一般情况下, 我们不允许匿名用户执行 delete 命令。

- 覆盖文件权限设置

格式: overwrite [yes/no] [real/anonymous/guest]

功能: 设置是否允许指定用户覆盖同名文件。默认是允许。

实例: overwrite no anonymous,guest: 为了更好地管理 FTP 服务器, 一般情况下, 我们不允许匿名用户覆盖同名文件。



- 文件改名权限设置

格式: `rename [yes/no] [real/anonymous/guest]`

功能: 设置是否允许指定用户使用 `rename` 命令来为文件改名。默认是允许。

实例: `delete no anonymous`: 为了更好地管理 FTP 服务器, 一般情况下, 我们不允许匿名用户执行 `rename` 命令改变文件名。而对有记录的匿名用户则适当的放宽, 允许他们使用改名命令。

- `chmod` 命令权限设置

格式: `chmod [yes/no] [real/anonymous/guest]`

功能: 设置是否允许指定用户使用 `chmod` 命令更改文件权限。默认是允许。

实例: `chmod no anonymous, guest`: 为了更好地管理 FTP 服务器, 一般情况下, 我们不允许匿名用户执行 `chmod` 命令更改文件权限。

- `umask` 命令权限

格式: `umask [yes/no] [real/anonymous/guest]`

功能: 设置是否允许指定用户使用 `umask` 命令。默认是允许。

实例: `umask no anonymous`: 为了更好地管理 FTP 服务器, 一般情况下, 我们不允许匿名用户执行 `umask` 命令。

- 用户上传目录

格式: `upload [根目录] [上载目录] [yes/no] [用户] [权限] [dirs/nodirs]`

功能: 对可以上载的目录进行更加详细的设置。

实例: `upload /home/ftpd * no`: 表示在子目录 `/home/ftpd` 下不允许上载;

`upload /home/ftpd /bin no`: 表示在子目录 `/home/ftpd/bin` 下不允许上载;

`upload /home/ftpd /etc no`: 表示在子目录 `/home/ftpd/etc` 下不允许上载;

`upload/home/ftpd/pub yes real 0644 dirs`: 允许服务器上的合法用户在子目录 `/home/ftpd/pub` 下能上载权限为 0644(也就是 `-rw-r--r--`) 的文件, 而且在这个目录下可以新建子目录。

`upload /home/ftpd /incoming yes real guest anonymous 0644 dirs`: 允许所有的用户在子目录 `/home/ftpd/incoming` 下能上载权限为 0644 的文件, 而且在这个目录下可以新建子目录。

- 虚拟目录

格式: `alias [目录别名] [目录名]`

功能: 为指定目录设置一个别名, 在切换目录时就可以使用较短的目录别名。

实例: `alias inc: /incoming`: 为子目录 `incoming` 设置一个别名 `inc`。

- 管理员的 E-mail 地址

格式: `email [guest 的 E-Mail 地址]`

功能: 只要在此设置系统管理员的 E-Mail 地址, FTP 服务器有问题或任何信息都要通知系统管理员。

实例: `email root@localhost`: 这里仅是一个示例, 实际上可以包含多个符合规范的 E-Mail 地址。

- 访问限制

格式: `deny [IP 地址/域名] [说明文件]`

功能：这个设置可以限制某些 IP 地址或域名的用户无法登入 FTP 服务器。

实例：deny \*.com.tw/etc/ftpd/deny.msg：设置凡是以“.com.tw”结束的域名，都禁止其访问。而将/etc/ftpd/deny.msg 的内容显示给用户看。

## 5. Wu-FTP 相关的其他一些命令的使用

### (1) 连接数字统计命令 ftpcount

ftpcount 命令可以十分清楚地统计出当前连接到 FTP 服务器上的用户数，并且同时列出上限。命令输出如下所示：

```
#ftpcount
Service class local      -   0   users   (20      maximum)
Service class remote     -   5   users   (100     maximum)
```

上例中显示属于 local(本地)的有 0 个人在线，上限为 20；属于 remote(远程)的有 5 个人在线，上限为 100。

### (2) 在线用户查看命令 ftpwho

ftpwho 命令可能查看当前连接的用户的具体情况。命令输入如下所示：

```
#ftpwho
Service class all:
ftp      12586   536 0    21:58 ? 00:00:00 ftpd: abc.com.cn :anonymous
ma       12557   532 0    21:58 ? 00:00:00 ftpd: localhost:ma:IDLE
-2 users (no maximum)
```

上例中显示 all 类有两个用户登录，并显示登录时间、来源和状态。

### (3) FTP 关闭文件生成命令 ftpshut

我们可以使用 ftpshut 命令生成一个在目录/etc/ftpaccess 中设置的 shut.msg 文件，用于关机设定。ftpshut 命令的格式为：

```
#ftpshut [-l<分钟>] [-d<分钟>] [关闭时间] ["警告信息"]
```

- -l<分钟> 指定在关闭 FTP 服务器功能前多少分钟时停止用户的连接；
- -d<分钟> 指定在关闭 FTP 服务器功能前多少分钟时切断用户连接；
- 关闭时间指定关闭 FTP 服务器的时间。例如 6:20 则写为 0620。如果要立即关闭，可以用 now；
- “警告信息” 指定断线之前显示给用户警告信息。

下面是 ftpshut 运行实例：

```
#ftpshut -l25 -d5 2300 "Warn: FTP server will shutdown!"
#cat /etc/shutmsg
2001 18 23 00 0025 0005
Warn:FTP server will shutdown!
```

例子中的 FTP 服务器将在 23:00 关闭，关闭前 25 分钟将拒绝用户登录，关闭前 5 分钟将断开所有连接，并给在线用户发送“Warn:FTP server will shutdown!”消息。

如果要立即关闭 FTP 服务器，则输入：

```
#ftpshut now
```

FTP 服务器关闭后要重新启动, 只要把目录/etc/shutmsg 下的这个文件删除, 并重新启动 FTP 服务器就可以继续 FTP 服务了。

### 3.4.2 典型例题分析

例 1 阅读以下说明, 回答问题 1~4, 将答案填入对应的答案栏内。

**【说明】**

某公司使用一台装有 Windows Server 2003 的 PC 服务器作为 WEB 服务器(文档的主目录为 D:\wwwroot)。为了能使 Web 管理员(其用户名为 webadmin)能够上传主页, 系统管理员在这台服务器上安装了 IIS 并配置了 FTP 服务。为了信息安全, 必须对这台服务器的 FTP 做一些控制。下面是一些要求, 请回答如何设置?

**【问题 1】**不使用 FTP 默认 TCP 端口 21 作为服务器端口, 而改用 TCP 端口 8089。

**【问题 2】**禁止匿名用户访问该台服务器上的 FTP 服务。

**【问题 3】**只能在 IP 地址为 210.45.12.31 的主机上上载或下载主页数据。

**【问题 4】**如果想要用户 webadmin 使用 FTP 登录时, 直接进入 WEB 服务器的文档主目录。

分析: 该题主要考查考生对 Windows Server 2003 下 FTP 服务器配置的掌握情况。该题比较简单, 这里就不作详细分析, 读者可参阅前文。

答案:

**【问题 1】**打开 FTP 站点属性窗口, 在【FTP 站点】选项卡的【TCP 端口】文本框中将“21”改为“8089”, 再重新启动 FTP 服务。

**【问题 2】**在【安全账户】选项卡中, 取消选中【允许匿名连接】, 即可禁止用户匿名访问该 FTP 站点。

**【问题 3】**在【目录安全性】选项卡中, 选中【拒绝访问】单选按钮, 单击【添加】按钮, 在弹出的对话框中, 选择【单机】单选按钮, 再在【IP 地址】文本框中输入 210.45.12.31。

**【问题 4】**新建一个别名为“webadmin”的虚拟目录, 其实际位置为 D:\wwwroot, 并将访问权限设置为【读取】和【写入】。

例 2 阅读以下说明, 回答问题 1~6, 将答案填入对应的答案栏内。

**【说明】**

在 Linux 下安装配置 Wu-FTP 服务, FTP 服务程序需要读取配置一些文件, 下面是几个 FTP 配置文件的主要内容:

/etc/ftpuser 文件的内容是:

```
root
uucp
news
bin
adm
nobody
```

```
lp
sync
shutdown
halt
mail
```

**/etc/ftphosts 文件的内容是:**

```
allow xyz *.abc.com.cn 210.102.0.0/16
deny tom *.hanker.com 131.222.154.0/24
```

**/etc/ftppass 文件的内容是:**

```
loginfails 5
class local real *
class remote anonymous guest *
limit remote 200 Any /etc/ftpd/toomany.msg
message /etc/ftpd/welcome.msg login
compress yes local remote
tar yes local remote
private yes
passwd-check rfc822 enforce
log commands real
log transfer anonymous guest inbound outbound
log transfer real inbound
shutdown /etc/ftpd/shut.msg
delete no anonymous,guest
overwrite no anonymous,guest
rename no anonymous
chmod no anonymous,guest
umask no anonymous
upload /home/ftpd * no
upload /home/ftpd /bin no
upload /home/ftpd /etc no
upload /home/ftpd /pub yes real 0644 dirs
upload /home/ftpd /incoming yes real guest anonymous 0644 dirs
alias in /incoming
email admin@abc.net.cn
email ferd@sina.com.cn
deny *.com.tw /etc/ftpd/deny.msg
```

**【问题 1】文件 etc/ftpuser 的作用是什么?**

**【问题 2】在文件/etc/ftppass 中, loginfails 5 一行的含义是什么?**

**【问题 3】该 FTP 最大在线人数是多少(不含本地登录)? 超过这个人数时, FTP 服务器如何响应客户机?**

**【问题 4】匿名用户登录时需要用什么密码验证?**

**【问题 5】如果限制 220.145.34.0/255.255.255.0 这一网段的用户访问该 FTP 服务器时,**



如何修改上述配置文件?

【问题6】当系统管理员输入: #ftpsht -l10 -d3 0430 "Warn:FTP server will shutdown!", 其功能是什么?

分析: 该题主要考查考生对 Linux 下 Wu-FTP 服务器配置的掌握情况。

问题1: 用于配置 Wu-FTP 服务器的主要有4个文件: /etc/ftpuser 文件用来指定某些用户登录不能登录本 FTP 服务器; /etc/ftpshosts 文件用来指定某些主机不能连接本 FTP 服务器; /etc/ftpconversions 文件主要定义用户从 FTP 服务器中下载文件时对文件进行格式转换的规则; /etc/ftppass 文件主要控制 FTP 的存取权限。

问题2: 在 /etc/ftppass 文件中, loginfails 用来设置用户的登录重试次数, 当用户密码输入错误次数超过设置值的就切断连接。

问题3: FTP 最大在线人数是通过 /etc/ftppass 文件中 limit 来定义的。其格式是:

limit [类别] [人数] [时间] [文件名]

因此, 本例中, 远程 FTP 登录的总人数不能超过 200 人, 若超过这个人数, 将给新连接的用户出示文件 /etc/ftpd/toomany.msg 的内容。

问题4: 匿名用户密码验证设置是通过 /etc/ftppass 文件中的 passwd-check 来定义的。其格式是:

```
passwd-check [none/trivial/rfc822] [enforce/warn]
```

none 表示不需做密码验证, 任何密码都可以登录; trivial 表示只要输入的密码中含有字符 "@" 就可以登录; rfc822 表示密码一定要符合 RFC822 中所规定的 E-Mail 地址才能登录; enforce 表示输入的密码不符合以上指定的格式就不允许登录; warn 表示密码不符合规定时只出现警告信息, 仍然能够登录。因此, 本例中, 匿名用户登录时必须要用符合 RFC822 中所规定的 E-Mail 地址作为密码才能登录。

问题5: 要禁止某些来自指定机器上的登录可以有两种方法, 一种方法就是在 /etc/ftppass 中设置 deny 命令, 另一种更加简单的方法就是在 /etc/ftpshosts 中写入要禁止的主机的 IP 地址或域名。

问题6: ftpshut 命令功能是生成一个在 /etc/ftppass 中设置的 shut.msg 文件, 该文件将决定什么时候将关闭 FTP 服务。ftpshut 命令的格式为:

```
#ftpshut <-lmin> <-dmin> time <warning-message>
```

- -lmin 指定在关闭 FTP 服务器功能前多少分钟时停止用户的连接;
- -dmin 指定在关闭 FTP 服务器功能前多少分钟时切断用户连接;
- time 指定关闭 FTP 服务器的时间。例如 6:20 则写为 0620;
- warning-message 指定断线之前显示给用户警告信息。

因此, #ftpshut -l10 -d3 0430 "Warn:FTP server will shutdown!" 就表示: 该 FTP 服务器将在 4:30 关闭, 关闭前 10 分钟将拒绝用户登录, 关闭前 3 分钟将断开所有连接, 并给用户发送 "Warn:FTP server will shutdown!" 的消息。

答案:

【问题1】/etc/ftpshosts 文件用来指定某些主机不能连接本地 FTP 服务器。

【问题2】用户登录重试次数为 5, 当用户连续 5 次输入错误密码是就切断连接。

【问题 3】200 人，若超过这个人数，将给新连接的用户出示文件/etc/ftpd/toomany.msg 的内容。

【问题 4】匿名用户登录时必须要用符合 RFC822 中所规定的 E-Mail 地址才能登录。

【问题 5】第一种方法是在/etc/ftpaccess 中添加“deny 194.66.78.0/24 /etc/ftpd/deny.msg”，第二种方法在/etc/ftphosts 中添加“deny \* 194.66.78.0/24”。

【问题 6】该 FTP 服务器将在 4:30 关闭，关闭前 10 分钟将拒绝用户登录，关闭前 3 分钟将断开所有连接，并给用户发送“Warn:FTP server will shutdown!”消息。

### 3.4.3 同步练习

1. 阅读以下说明，回答问题 1~4，将答案填入对应的答案栏内。

【说明】

某公司使用一台装有 Windows Server 2003 的 PC 服务器作为 FTP 服务器，主要用于内部文件下载。该公司的网络地址是 192.168.10.0/24 这个 C 类地址，内部文件都存放在“D:\公用文件”下，另外每个用户都在该服务器上有一个账号和自己的主文件夹(主文件夹都不在“D:\公用文件”下)。

【问题 1】若该公司内部所有的用户使用匿名用户就可以下载内部文件，FTP 站点主目录设置成什么？如何设置？

【问题 2】为保证外网的用户不能访问该 FTP 站点，如何设置？

【问题 3】由于该服务器还提供其他服务，必须要限制最大在线人数为 100，如何实现这一功能？

【问题 4】如果想要让每个用户使用自己的账号登录到 FTP 该服务器时，就直接进入自己的主文件夹，如何实现这一功能？

2. 阅读以下说明，回答问题 1~8，将答案填入对应的答案栏内。

【说明】

在 Linux 下安装配置 Wu-FTP 服务，FTP 服务程序需要读取配置一些文件，下面是几个 FTP 配置文件的主要内容。

/etc/ftpuser 文件的内容是：

```
root
uucp
news
bin
adm
nobody
lp
sync
shutdown
halt
mail
```

/etc/ftphosts 文件的内容是：

```
allow xyz *.abc.com.cn 210.102.0.0/16
deny tom *.hanker.com 131.222.154.0/24
```

/etc/ftppass 文件的内容是:

```
loginfails 5
class local real *
class remote anonymous guest *
limit remote 100 Any /etc/ftpd/toomany.msg
message /etc/ftpd/welcome.msg login
compress yes local remote
tar yes local remote
private yes
passwd-check _____ (1)
log commands real
log transfer anonymous guest inbound outbound
log transfer real inbound
shutdown /etc/ftpd/shut.msg
delete no anonymous,guest
overwrite no anonymous,guest
rename no anonymous
chmod no anonymous,guest
umask no anonymous
upload /home/ftpd * no
upload /home/ftpd /bin no
upload /home/ftpd /etc no
upload /home/ftpd /pub yes real 0644 dirs
upload /home/ftpd /incoming yes real guest anonymous 0644 dirs
alias in /incoming
_____ (2)
deny *.com.tw /etc/ftpd/deny.msg
```

【问题1】该服务器安装了 Oracle 服务器，创建了一个名为 Oracle 的用户，但不能让该用户登录到 FTP 站点，如何设置？

【问题2】该 FTP 最大在线人数是多少(不含本地登录)？超过此人数时 FTP 服务器如何响应客户机？

【问题3】匿名用户登录时，必须用带有“@”字符的密码来验证，否则无法登录，则(1)处该填写什么？

【问题4】该 FTP 站点的管理员的电子邮件地址是 fred@abc.com.cn，若服务器出现问题时，就通过这个电子邮件地址通知系统管理员，则(2)处该填写什么？

【问题5】如果发现网段 194.66.78.0 中有黑客在攻击该 FTP 站点，如何限制该网段内用户再次访问？请说出两种方法。

【问题6】系统管理员输入命令 #ftpwho，将会显示什么内容？

【问题7】系统管理员输入命令 #ftpcount，将会显示什么内容？

【问题8】系统管理员想立即关闭 FTP 服务，该输入什么命令？

### 3.4.4 同步练习参考答案

1.

【问题 1】主目录应设置为“D:\公用文件”，操作步骤是：在 FTP 站点的属性窗口中，选择【主目录】选项卡，选中【此计算机的目录】单选按钮，在【FTP 站点目录】选项区域中，单击【浏览】按钮，选择“D:\公用文件”，或者直接输入“D:\公用文件”。

【问题 2】设置目录安全性的具体操作步骤是：在 FTP 站点的属性窗口中，选择【目录安全性】选项卡，选中【拒绝访问】单选按钮，单击【添加】按钮，在【授权以下访问】对话框中，选择【一组计算机】单选按钮，在【网络标识】文本框中输入 192.168.10.0，在【子网掩码】文本框中输入 255.255.255.0。

【问题 3】设置最大连接数，具体操作步骤是：在 FTP 站点的属性窗口中，选择【FTP 站点】选项卡，选择【限制到】单选按钮，并在后面填入 100。

【问题 4】在 FTP 站点中，为每一个用户建立和用户名相同的虚拟目录，其真实路径指向该用户的主文件夹，并将权限设置为“读取”和“写入”。

2.

【问题 1】在/etc/ftpuser 文件添加一行，内容为 Oracle

【问题 2】100 个，超过时将把/etc/ftpd/toomany.msg 文件中的内容出示给用户。

【问题 3】trivial enforce

【问题 4】email fred@abc.com.cn

【问题 5】第一种方法是在/etc/ftpaccess 中添加“deny 220.145.34.0/24 /etc/ftpd/deny.msg”，第二种方法是在/etc/ftpshosts 中添加“deny \* 220.145.34.0/24”（因为 220.145.34.0 是一个 C 类地址，子网掩码是 24 位，即 255.255.255.0）

【问题 6】查看当前连接的用户的具体情况。

【问题 7】统计出当前连接到 FTP 服务器上的用户数目，并且同时列出其上限。

【问题 8】#ftpsht now

## 3.5 WWW 服务器配置

### 3.5.1 考点辅导

#### 3.5.1.1 Red Flag Linux 下 Apache Web 服务器的配置

##### 1. 启动 rfapache

rfapache 配置工具需要在 KDE 环境下以 root 权限运行。非 root 用户虽然允许运行和使用配置工具，但由于没有权限修改配置文件，所以即使在配置工具中修改了选项也无法保存和生效。启动 rfapache 配置工具有以下三种方式：

(1) 在系统菜单中选择【系统】|【控制面板】，打开控制面板，在【网络服务配置】



标签页中，双击【Apache 配置工具】：

(2) 在系统主菜单中选择【管理工具】|【Apache 配置工具】；

(3) 在运行命令行或 shell 提示符下直接输入 rfapache。

rfapache 的配置主界面窗口左侧是 Apache Server 的控制台树，显示了服务器主机中已建的主机站点和目录的树状结构；窗口右侧从上到下依次为列表显示区、配置文件编辑器、配置文件跳转器和消息显示窗口；在左侧的控制台树中选某节点时，列表显示区中将出现该节点中的内容，可以按名称、类型或路径名排序。如果选中的是一个目录，则显示该目录中的所有子目录和文件；管理员可以在配置文件编辑器中手工修改配置文件，并保存。消息显示窗口显示的是 Apache 服务器启动、重启、停止或校验配置文件等的输出信息。

## 2. 启动、停止和重新启动 Apache 服务

打开 Apache 配置工具 rfapache，在主界面窗口中：

- 选择菜单栏中的【操作】|【启动】，启动 httpd 服务；
- 选择菜单栏中的【操作】|【停止】，停止 httpd 服务；
- 选择菜单栏中的【操作】|【重启】，重新启动 httpd 服务。

如果 httpd 服务已经启动，那么菜单项【操作】|【启动】不可用；如果 httpd 服务没有启动，那么菜单项【操作】|【停止】和【操作】|【重启】不可用。操作结果的输出信息将显示在消息窗口中。

管理员也可以在命令行终端下启动、停止和重新启动 Apache，命令分别是：

```
#/etc/init.d/httpd start  
#/etc/init.d/httpd stop  
#/etc/init.d/httpd restart
```

## 3. 添加和删除虚拟主机

虚拟主机是指在一个单一的服务器上维护多个 Web 站点，并且使用主机别名来区别它们。这样用户就可以在单一的 Web 服务器上拥有多个的 Web 站点，并通过它们各自的域名对这些站点进行访问，而无须用户了解任何其他路径信息。

随着 Internet 上的 Web 站点数目逐渐增多，在一台服务器上有效托管多个 Web 站点的能力已经成为第一流 Web 服务器引擎的关键特性。Apache 提供了对虚拟主机的完全支持。虚拟主机一般有两种形式：“基于名字”和“基于 IP”。

### (1) 添加虚拟主机

Apache 配置工具中提供了一个虚拟主机的创建向导。打开 rfapache，在菜单中选择【操作】|【添加虚拟主机】，或者单击工具栏中的【添加虚拟主机】按钮，按照【虚拟主机创建向导】中的提示完成操作。

通过这个向导，管理员可以定义虚拟主机的主机名、IP 地址和端口、主目录、规划用户的访问权限等，在向导的最后，还列出了新建虚拟主机的概要信息。创建虚拟主机时，需要保证所创建的虚拟服务器名称能够在 DNS 中正确解析。

当设置出现下列问题的时候，工具将给出错误提示，提示重新设置：

- 对于“基于名称”的虚拟主机，设置的主机名已经被其他虚拟主机使用；
- 对于“基于 IP”的虚拟主机，选择的 IP 地址(端口)已经被其他虚拟主机使用；

- 指定的主目录不存在或不是一个合法的路径。

## (2) 删除虚拟主机

在 rfapache 配置工具主窗口左侧的控制台树中, 选择需要删除的虚拟主机名。单击菜单中的【操作】|【删除】, 或单击工具栏中的【删除】按钮, 当被询问是否确认要删除该主机时, 单击【确定】即可。

## 4. 添加和删除虚拟目录

虚拟目录的概念源于 Alias 和 ScriptAlias 指令, 一般称为“别名”。这样的指令可以将一个 URL 以非标准方式映射到一个目录文件名, 也就是说可以将文档存储在服务器定义的主目录以外的位置。通过别名访问时, 要在别名后加一个斜线后缀“/”。

### (1) 创建虚拟目录

在 rfapache 配置工具主窗口左侧的控制台树中, 选择虚拟目录要添加的位置(默认主机或者是虚拟主机)。单击菜单中的【操作】|【添加虚拟目录】, 或者单击工具栏中的【添加虚拟目录】按钮, 在弹出的【虚拟目录创建向导】中, 根据提示创建一个新的虚拟目录。利用这个向导, 管理员可以定义虚拟目录的别名、目录的路径、规划用户的访问权限等; 在向导的最后, 列出了新建虚拟目录的概要信息。

当设置出现下列问题的时候, 工具将给出错误提示, 提示重新设置:

- 设置的别名已经存在;
- 设置的目录路径不合法;
- 设置的目录已经被其他别名映射。

### (2) 删除虚拟目录

在 rfapache 配置工具主窗口左侧的树状结构中, 选择需要删除的虚拟目录。单击菜单中的【操作】|【删除】, 或单击工具栏中的【删除】按钮, 当被询问是否确认要删除该虚拟目录时, 单击【确定】即可。

## 5. 设置属性

可以在配置工具 rfapache 中设置“默认主机”、“虚拟主机”和“虚拟目录”的属性。

在 rfapache 配置工具主窗口左侧的控制台树中, 选择需要查看或设置属性的主机或目录, 单击菜单中的【操作】|【设置属性】, 或者单击工具栏中的【设置属性】按钮, 也可以右击, 从快捷菜单中选择【设置属性】, 在弹出的属性设置窗口中查看或修改相应的属性。属性设置窗口中包括多个配置选项卡, 具有相当多的选项可供设置, 分别说明如下:

(1) 站点属性: 使用站点属性选项卡设置站点的标识参数和日志信息等, 只有默认主机和虚拟主机有此选项卡。主要包括: ① 站点属性: 站点名称(配置项: ServerName)、管理员 E-Mail(配置项: ServerAdmin)、IP 地址和 TCP 端口; ② 错误日志: 日志位置(配置项: ErrorLog)、日志级别(配置项: LogLevel); ③ 自定义日志: 日志位置(配置项: Customlog)、日志格式、详细格式(配置项: LogFormat)。

(2) 主目录: 使用此选项卡修改主目录的路径(配置项: DocumentRoot)、设置主目录的执行属性(配置项: Options)和目录别名(配置项: Alias)。

(3) 访问许可: 用来根据 IP 地址或域名等来授权或者禁止对资源的访问。访问顺序(配置项: Order), 基本上有下面两种形式: 先禁止后允许和先允许后禁止; 允许访问列表(配



置项: Allow from); 禁止访问列表(配置项: Deny from)。

(4) 默认文档: 使用此选项卡定义站点的默认页面。默认文档的配置项是 DirectoryIndex。在这里设置请求指定目录时该目录的索引文件, 用户可以定义多个这样的索引文件, 若要添加新的默认文档, 单击【添加】。

(5) 错误信息: 错误信息的配置项是 ErrorDocument。如果 Apache 在处理用户请求时遇到错误, 它将按照配置显示一个标准错误页; 给出 HTTP 响应代码; 使用 ErrorDocument 指令并针对标准 HTTP 错误来自定义成用户的错误响应, 以使用户更容易理解。针对虚拟主机设置的错误信息会继承默认主机中的值; 同样, 虚拟目录的默认文档也会继承虚拟主机(或默认主机)中的值。如果要添加新的自定义错误消息, 单击【添加】; 如果要更改某一错误消息的属性, 单击【编辑】; 如果要删除某一自定义错误消息, 单击【删除】。

(6) 性能: 用来设置一些和 Apache 运行性能有关的配置项。只有“默认主机”包含此选项卡。保持连接(配置项: KeepAlive)、保持连接时间(配置项: KeepAliveTimeout)、最大请求保持数(配置项: MaxKeepAliveRequests)、连接超时(配置项: Timeout)、初始化最大进程数(配置项: StartServers)、最小空闲进程数(配置项: MinSpareServers)、最大空闲进程数(配置项: MaxSpareServers)、单进程最大请求数(配置项: MaxRequestsPerChild)、最大连接数(配置项: MaxClients)。

(7) 杂项: 用来设置一些其他的常用且很重要的配置项。只有“默认主机”包含此选项卡。服务器根目录(配置项: ServerRoot)、服务 PID 文件(配置项: PidFile)、服务 LOCK 文件(配置项: LockFile)、用户名(配置项: User)、组名(配置项: Group)。

### 3.5.1.2 Linux 下 Apache Web 服务器的安装与配置

#### 1. Apache Web 服务器的安装

如果用户在安装 Linux 时一并安装了 Apache Web 服务器, 就不需要另行安装。如果用户不能确定是否已经安装了 Apache Web 服务器, 可以通过执行以下命令检查:

```
#rpm -qa |grep apache
apache-1.3.20-16          //若出现此行, 则表示已经安装了 Apache 主程序
apache-0.8.1-1           //若出现此行, 则表示已经安装了 Apache 配置文件
apache-devel-1.3.20-16   //若出现此行, 则表示已经安装了 Apache 开发工具软件
apache-manual-1.3.20-16  //若出现此行, 则表示已经安装了 Apache 说明文件
```

如果用户发觉系统未安装 Apache Web 服务器, 可以在网上下载 Apache Web 服务器的安装包, 也可以 Red Hat Linux 安装盘中找到 Apache Web 服务器安装包。安装命令是:

```
#rpm -ivh apache*.rpm          //安装 Apache Web 服务器
```

如果用户想从旧版本的 Apache Web 服务器升级到新的版本, 只需把执行参数“-i”改为“-U”即可:

```
#rpm -Uvh apache*.rpm          //更新 Apache Web 服务器
```

#### 2. Apache Web 服务器配置

如果安装时未指定安装目录, Apache 服务器的设置文件位于 /usr/local/apache/conf/ 目录

下,传统上使用三个配置文件——httpd.conf、access.conf 和 srm.conf 来配置 Apache 服务器的行为。

httpd.conf 提供了最基本的服务器配置,是对守护程序 httpd 的运行方式的技术描述; srm.conf 是服务器的资源映射文件,告诉服务器各种文件的 MIME 类型,以及如何支持这些文件; access.conf 用于配置服务器的访问权限,控制不同用户和计算机的访问限制。

事实上当前版本的 Apache 将原来 httpd.conf、srm.conf 与 access.conf 中的所有配置参数均放在了一个配置文件 httpd.conf 中,只是出于与以前的版本兼容的原因(使用这三个设置文件的方式来源于 NCSA-httpd),才使用三个配置文件。而提供的 access.conf 和 srm.conf 文件中没有具体的设置。

由于在新版本的 Apache 中,所有的设置都被放在了 httpd.conf 中,而 access.conf 和 srm.conf 文件中没有具体的设置。以下使用默认提供的 httpd.conf 为例,解释 Apache 服务器的各个设置选项。然而不必因为它提供设置的参数太多而烦恼,基本上这些参数都很明确,也可以不加改动运行 Apache 服务器。但如果需要调整 Apache 服务器的性能,以及增加对某种特性的支持,就需要了解这些设置参数的含义。下面介绍几个常用的参数。

#### (1) ServerType

ServerType 是用来定义服务器的启动方式,默认值为独立方式 standalone, httpd 服务器将由其本身启动,并驻留在主机中监视连接请求。在 Linux 下将在启动文件 /etc/rc.d/rc.local/init.d/apache 中自动启动 Web 服务器,这种方式是推荐设置。Apache 服务器工作在 standalone 方式时,代码为:

```
ServerType standalone
```

启动 Apache 服务器的另一种方式是 inetd 方式,使用超级服务器 inetd 监视连接请求并启动服务器。Apache 服务器工作在 inetd 方式时,代码为:

```
ServerType inetd
```

当需要使用 inetd 启动方式时,需要更改某些设置,从而屏蔽/etc/rc.d/rc.local/init.d /apache 文件。考虑到这种运行方式很少使用,这里就不作详细介绍了。

两种方式的区别是独立方式是由服务器自身管理自己的启动进程,这样在启动时能立即启动服务器的多个副本,每个副本都驻留在内存中,一有连接请求不需要生成子进程就可以立即进行处理,对于客户浏览器的请求反应更快、性能更高。而 inetd 方式要由 inetd 发现有连接请求后才去启动 http 服务器,由于 inetd 要监听太多的端口,因此反应较慢、效率较低,但节约了没有连接请求时 Web 服务器占用的资源。因此 inetd 方式只用于偶尔被访问并且不要求访问速度的服务器上。事实上 inetd 方式不适合 http 的突发和多连接的特性,因为一个页面可能包含多个图像,而每个图像都会引起一个连接请求,即使虽然访问人数较少,但瞬间的连接请求并不少,这就受到 inetd 性能的限制,甚至会影响由 inetd 启动的其他服务器程序。

#### (2) ServerRoot

ServerRoot 用于指定守护进程 httpd 的运行目录, httpd 在启动之后将自动将进程的当前目录改变为这个目录,因此如果设置文件中指定的文件或目录是相对路径,那么真实路径就位于这个 ServerRoot 定义的路径之下。



### (3) Port

Port 定义了 Standalone 模式下 httpd 守护进程使用的端口, 标准端口是 80。这个选项只对于以独立方式启动的服务器才有效, 对于以 inetd 方式启动的服务器, 则在 inetd.conf 中定义使用哪个端口。

### (4) ServerAdmin

ServerAdmin 用于配置 WWW 服务器的管理员的 E-Mail 地址, 这将在 HTTP 服务出现错误的条件下返回给浏览器, 以便让 Web 使用者和管理员联系, 及时报告错误。习惯上使用服务器上的 webmaster 作为 WWW 服务器的管理员, 通过邮件服务器的别名机制, 将发送到 webmaster 的电子邮件发送给真正的 Web 管理员。

### (5) ServerName

默认情况下, 并不需要指定这个 ServerName 参数, 服务器将自动通过名称解析过程来获得自己的名称, 但如果服务器的名称解析有问题(通常为反向解析不正确), 或者没有正式的 DNS 名称, 也可以在这里指定 IP 地址。当 ServerName 设置不正确的时候, 服务器无法正常启动。

### (6) DocumentRoot

DocumentRoot 定义这个服务器对外发布的超文本文档所存放的路径, 客户程序请求的 URL 就被映射为这个目录下的网页文件。这个目录下的子目录, 以及使用符号连接指出的文件和目录都能被浏览器访问, 只是要在 URL 上使用同样的相对目录名。

注意, 符号连接虽然逻辑上位于根文档目录之下, 但实际上可以位于计算机上的任意目录中, 因此可以使客户程序能访问那些根文档目录之外的目录, 这在增加了灵活性的同时却减少了安全性。Apache 在目录的访问控制中提供了 FollowSymLinks 选项来打开或关闭支持符号连接的特性。

### (7) UserDir

当在一台 Linux 上运行 Apache 服务器时, 这台计算机上的所有用户都可以有自己的网页路径, 形如 http://example.abc.com.cn/~user, 使用波浪符号加上用户名就可以映射到用户自己的网页目录上。映射目录为用户个人主目录下的一个子目录, 其名称就用 UserDir 这个参数进行定义, 默认为 public\_html。如果不想为正式的用户提供网页服务, 使用 DISABLED 作为 UserDir 的参数即可。

### (8) DirectoryIndex

很多情况下, URL 中并没有指定文档的名称, 而只是给出了一个目录名。那么 Apache 服务器就自动返回这个目录下由 DirectoryIndex 定义的文件, 当然可以指定多个文件名称, 系统会在这个目录下按顺序搜索。当所有由 DirectoryIndex 指定的文件都不存在时, Apache 服务器可以根据系统设置, 生成这个目录下的所有文件列表, 提供用户选择。此时该目录的访问控制选项中的 Indexes 选项(Options Indexes)必须打开, 以使得服务器能够生成目录列表, 否则 Apache 将拒绝访问。

### (9) Alias

Alias 参数用于将 URL 与服务器文件系统中的真实位置进行直接映射(虚拟目录), 一般的文档将在 DocumentRoot 中进行查询, 然而使用 Alias 定义的路径将直接映射到相应目录下, 而不再到 DocumentRoot 下面进行查询。因此 Alias 可以用来映射一些公用文件的路径,

例如保存了各种常用图标的 `icons` 路径。这样使得除了使用符号连接之外, 文档根目录 (`DocumentRoot`) 外的目录也可以通过使用了 `Alias` 映射, 提供给浏览器访问。定义好映射的路径之后, 应该需要使用 `Directory` 语句设置访问限制。

`ScriptAlias` 也是用于 URL 路径的映射, 但与 `Alias` 的不同在于, `ScriptAlias` 是用于映射 CGI 程序的路径, 这个路径下的文件都被定义为 CGI 程序, 通过执行它们来获得结果, 而非由服务器直接返回其内容。默认情况下 CGI 程序使用 `cgi-bin` 目录作为虚拟路径。

#### (10) ErrorDocument

如果发生了某些意外情况, 例如用户请求的网页不存在, 或者没有访问权限时, 服务器将生成一个错误代码, 同时也将回应用户浏览器一个标识错误的网页。

`ErrorDocument` 就用于设置当出现哪个错误时应该回应用户浏览器哪些内容, `ErrorDocument` 的第一个参数为错误的序号, 第二个参数为回应的数据, 可以是简单的文本、本地网页、本地 CGI 程序以及远程主机上的网页。例如:

```
ErrorDocument 404 /missing.html
ErrorDocument 404 /cgi-bin/missing_handler.pl
ErrorDocument 402 http://some.other_server.com/subscription_info.html
```

#### (11) 虚拟主机

虚拟主机位于一台 Web 服务器上, 可以为多个单独域名提供 Web 服务, 并且每个域名都完全独立, 包括具有完全独立的文档目录结构及设置, 这样域名之间完全独立, 不但使用每个域名访问到的内容完全独立, 并且使用另一个域名无法访问其他域名提供的网页内容。

在 Apache Web 服务器中, 有两种设定虚拟主机的方式: 一种是 IP-Based(基于 IP 方式), 另一种是 Name-Based(基于域名方式)。下面是一个基于域名方式的配置示例:

```
NameVirtualHost 192.168.10.101
<VirtualHost 192.168.10.101>
    ServerAdmin webmaster@company1.com.cn
    DocumentRoot /www/htdocs/company1
    ServerName www.company1.com.cn
    ErrorLog logs/company1.com.cn -error_log
    CustomLog logs/ company1.com.cn-access_log common
</VirtualHost>
```

其中 `NameVirtualHost` 参数用来指定虚拟主机使用的 IP 地址(192.168.10.101), 这个 IP 地址将对应多个 DNS 名字, 如果 Apache 使用了 `Listen` 参数控制了多个端口, 那么就可以在这里加上端口号以进一步进行区分对不同端口的不同连接请求。

`<VirtualHost 192.168.10.101>.....</VirtualHost>` 之间的语句是用来设置虚拟主机相关参数, 如管理员的邮箱(`webmaster@company1.com.cn`)、文档主目录(`/www/htdocs/company1`)、服务器的域名(`www.company1.com.cn`)、错误日志(`logs/company1.com.cn -error_log`)和访问日志(`logs/ company1.com.cn-access_log common`)的位置等。

### 3. 启动、停止和重新启动 Apache Web 服务器

Apache Web 服务器守护程序为 `httpd`, 当 Apache Web 服务器运行在 `standalone`(独立)

模式下, 可以通过 `httpd` 来启动、停止和重新启动 Apache Web 服务器。其命令分别是:  
`#/etc/init.d/httpd start`、`#/etc/init.d/httpd stop`、`#/etc/init.d/httpd restart`。

如果设定 Apache Web 服务器在计算机启动时自动启动或不启动, 可以使用 `ntsysv` 命令将它加到引导程序中, 也可以通过 `chkconfig` 命令来设定, 该命令格式是:

```
chkconfig [--level <运行级>] <名字> [on|off]
```

例如我们希望计算机启动运行级别 3、5 时启动 Apache Web 服务器, 则命令为:

```
#chkconfig --level 3 5 httpd on
```

再如我们希望计算机启动运行级别 2 时不启动 Apache Web 服务器, 则命令为:

```
#chkconfig --level 2 httpd off
```

如果希望在任何运行级别下启动时都不启动 Apache Web 服务器, 只需将 “[--level <运行级>]” 不设定就可以了, 即:

```
#chkconfig httpd on  
#chkconfig httpd off
```

### 3.5.2 典型例题分析

例 阅读以下说明, 回答问题 1~6, 将答案填入对应的答案栏内。

#### 【说明】

在 Linux 下安装配置 Apache 服务, Apache 服务程序 `httpd` 启动时需要读取配置文件 `httpd.conf`, 以下是一个 `httpd.conf` 配置文件的片断:

```
## httpd.conf -- Apache HTTP server configuration file
```

```
### Section 1: Global Environment
```

```
ServerType standalone
```

```
ServerRoot "/etc/httpd"
```

```
Timeout 300
```

```
KeepAlive On
```

```
MaxKeepAliveRequests 100
```

```
KeepAliveTimeout 15
```

```
MaxClients 150
```

```
### Section 2: 'Main' server configuration
```

```
Port 80
```

```
User apache
```

```
Group apache
```

```
ServerAdmin webmaster@abc.com.cn
```

```
ServerName www.abc.com.cn
```

```
DocumentRoot "/var/www/html"
```

```
UserDir public_html
```

```
DirectoryIndex index.html
```

```
Alias /jianji "/home/zhang/jianji"
ScriptAlias /cgi-bin/ "/var/www/cgi-bin/"
ErrorDocument 404 /missing.html

### Section 3: Virtual Hosts
NameVirtualHost 192.168.10.101
<VirtualHost 192.168.10.101>
    ServerAdmin webmaster@abc.com.cn
    DocumentRoot /www/htdocs/abc
    ServerName markert.abc.com.cn
    ErrorLog logs/host.some_domain.com-error_log
    CustomLog logs/host.some_domain.com-access_log common
</VirtualHost>
```

【问题 1】该 Web 服务器的运行方式是什么？

【问题 2】该 Web 服务器文档主目录是什么？

【问题 3】当用户在浏览器中输入 `http://192.168.10.100` 时显示了主页，那么该主页的文件名是什么？

【问题 4】`httpd.conf` 文件中 `Alias /jianji "/home/zhang/jianji"` 一行的含义是什么？

【问题 5】`httpd.conf` 文件中阴影部分的作用是什么？

【问题 6】当修改 `httpd.conf` 文件后，如何使配置文件生效？(不重新启动计算机)

分析：该题主要考查考生对 Linux 下配置 Apache 服务器的掌握情况。

传统上，使用三个配置文件 `httpd.conf`，`access.conf` 和 `srm.conf` 来配置 Apache 服务器的行为。事实上当前版本的 Apache 将原来 `httpd.conf`、`srm.conf` 与 `access.conf` 中的所有配置参数均放在了一个配置文件 `httpd.conf` 中，只是为了与以前的版本兼容的原因才使用三个配置文件。由于 Apache 的配置参数很多，无法在例子中全部涉及到，这里要节选一些常见的参数作讲解。

问题 1: Apache 服务器有两种运行方式，一种是独立方式(`standalone`)，这是 Apache 服务器的默认运行方式。在这种方式中，`httpd` 服务器将由其本身启动，并驻留在主机中监视连接请求。另一种是 `inetd` 方式，它使用超级服务器 `inetd` 监视连接请求并启动服务器。Apache 服务器的运行方式是通过 `ServerType` 参数指定的，因此，例子中的服务器的运行方式是独立方式(`standalone`)。

问题 2: 文档主目录是 Web 站点发布树的顶点，也是站点访问的起点。在 Apache 服务中，通过 `DocumentRoot` 参数来定义这个服务器对外发布的超文本文档存放的路径，客户程序请求的 URL 就被映射为这个目录下的网页文件。因此，例中的服务器的文档主目录是 `"/var/www/html"`。

问题 3: 该问题主要是考查索引文件(默认文档)的设置。很多情况下，URL 中并没有指定文档的名称，而只是给出了一个目录名。那么 Apache 服务器就自动返回到这个目录下由 `DirectoryIndex` 定义的文件，当然可以指定多个文件名称，系统会按顺序搜索。当所有由 `DirectoryIndex` 指定的文件都不存在时，Apache 服务器可以根据系统设置，生成这个目录下的所有文件列表，供用户选择。此时该目录的访问控制选项中的 `Indexes` 选项(`Options`



Indexes)必须打开,使得服务器能够生成目录列表,否则 Apache 将拒绝访问。例子中 DirectoryIndex 只定义了 index.html,因此我们看到主页文件名为 index.html。

问题 4: Alias 参数用于将 URL 与服务器文件系统中的真实位置进行直接映射(虚拟目录),一般的文档将在 DocumentRoot 中进行查询,然而使用 Alias 定义的路径将直接映射到相应目录下,而不再到 DocumentRoot 下面进行查询。因此, Alias /jianji "/home/zhang/jianji" 一行的含义是建立一个虚拟目录 /jianji,其真实路径是 /home/zhang/jianji。

问题 5: 其作用是建立一个域名为 markert.abc.com.cn 的虚拟 Web 服务器(虚拟主机),并指定相应的参数。NameVirtualHost 参数用来指定虚拟主机使用的 IP 地址,<VirtualHost 192.168.10.101>...</VirtualHost>之间的参数是用来指定使用 NameVirtualHost 参数指定的虚拟主机相关设置,如管理员的邮箱、文档主目录、服务器的域名、错误日志和访问日志的位置等。

问题 6: 要使修改后的配置文件生效,必须重新启动 Apache 服务器。Apache 服务器在独立方式(standalone)运行时,可通过服务器守护程序为 httpd 来重新启动它,其命令是:

```
#/etc/init.d/httpd restart
```

答案:

【问题 1】独立方式(standalone)

【问题 2】/var/www/html

【问题 3】index.html

【问题 4】建立一个虚拟目录/jianji,其真实路径是/home/zhang/jianji。

【问题 5】建立一个域名为 markert.abc.com.cn 的虚拟 Web 服务器(虚拟主机),并指定相应的参数。

【问题 6】#/etc/init.d/httpd restart

### 3.5.3 同步练习

1. 在 Red Flag Linux 中可以通过什么命令启动 Apache 配置工具?
2. 在 Red Flag Linux 中如何通过启动 Apache 服务?请说出两种方式。
3. 阅读以下说明,回答问题 1~6,将答案填入对应的答案栏内。

【说明】

有一台 Linux 服务器,配置了 Apache 服务,该服务器运行于独立方式下,监听端口是 80,工作目录为 "/usr/local",主文件目录为 "/www/",用户文档目录为 public\_html,当用户请求一个不存在的文档时,将文档/missing.html 来回应用户浏览器,建立了一个虚拟目录,需要建立一个虚拟目录/icons/,其真实路径是/var/www/icons。以下是 httpd.conf 配置文件的片断:

```
## httpd.conf -- Apache HTTP server configuration file

### Section 1: Global Environment
ServerType _____ (1)
```

```

ServerRoot " _____ (2) "
Timeout 300
KeepAlive On
MaxKeepAliveRequests 100
KeepAliveTimeout 15
MaxClients 150

### Section 2: 'Main' server configuration
Port 80
User apache
Group apache
ServerAdmin root@localhost
ServerName localhost
DocumentRoot " _____ (3) "
UserDir public_html
DirectoryIndex index.html index.htm index.php index.php4
_____ (4)
ScriptAlias /cgi-bin/ "/var/www/cgi-bin/"
ErrorDocument _____ (5)

```

【问题 1】(1)处填什么内容?

【问题 2】(2)处填什么内容?

【问题 3】(3)处填什么内容?

【问题 4】在(4)处需要建立一个名称为/icons/的虚拟目录,则应填什么内容?

【问题 5】(5)处填什么内容?

【问题 6】httpd.conf 文件中阴影一行的含义是什么?

### 3.5.4 同步练习参考答案

1. 在 KDE 环境下以 root 权限来运行 DNS 配置工具 rfapache。

2.

方法一: 使用命令行终端来启动, 命令如下:

```
#/etc/init.d/httpd start
```

方法二: 使用菜单命令来启动: 在控制台菜单中选择【操作】|【启动】命令。

3.

【问题 1】standalone

【问题 2】/usr/local

【问题 3】/www/

【问题 4】Alias /icons/ "/var/www/icons/"

【问题 5】404 /missing.htm

【问题 6】该行是指定索引文件(默认文档)及搜索顺序, 即当用户访问一个目录时没有指定文件名时, 依次寻找 index.htm、index.htm、index.php、index.php 文件, 并用它来响应

客户的请求。

## 3.6 代理服务器配置

### 3.6.1 考点辅导

#### 3.6.1.1 代理服务器的基础知识

##### 1. 代理服务器的概念和功能

随着 Internet 技术的迅速发展,越来越多的个人计算机接入了 Internet,很多公司也将自己公司的局域网接入了 Internet。如何快速地访问 Internet 站点,提高网络的安全性,成为了当今的热门话题。在这种情况下,代理服务器便应运而生了。

##### (1) 代理服务器的概念

代理服务器(Proxy Server)是个人网络和 Internet 服务商之间的中间代理机构,它负责转发合法的网络信息,对转发进行控制和登记。代理服务器作为连接 Internet 与 Intranet 的桥梁,在实际应用中发挥着极其重要的作用。它可用于多个目的,最基本的功能是连接,此外还提供安全性、缓存、内容过滤、访问控制管理等功能。代理服务器,顾名思义,就是代理网络服务的机构。局域网上不能直接上网的机器将上网请求(比如说,浏览某个主页)发给能够直接上网的代理服务器,由代理服务器代理完成这个上网请求,将请求者所要浏览的主页调入代理服务器的缓存;然后将这个页面传给请求者。这样,局域网上的机器就像能够直接访问网络一样。并且,代理服务器还可以进行一些网站的过滤和控制的工作,这样就实现了控制和节省上网费用的目的。

代理服务器能够让多台没有 IP 地址的电脑利用其代理功能高速、安全地访问互联网资源。当代理服务器客户端发出一个对外的资源访问请求,该请求先被代理服务器识别并代为向外请求访问资源。由于一般代理服务器拥有较大的带宽、较高的性能,并且能够智能化地缓存已浏览或未浏览的网站内容,因此,在一定条件下,客户端通过代理服务器能更快速地访问网络资源。代理服务器应用的常见例子:拥有上百台电脑的局域网通过一台能够访问外部网络资源的代理服务器访问外部互联网。

##### (2) 代理服务器的功能

##### ① 作为防火墙

代理服务器可以保护局域网的安全,起防火墙的作用。通过设置防火墙,为公司内部的网络提供安全边界,防止外界的入侵。

##### ② 实现网络地址转换

网络地址转换(NAT, Network Address Translation)最主要的功能是实现 IP 地址的多个对应多个或者多个对应一个的映射,从而节约 IP 地址空间。基于这种功能,通过代理服务器访问 Internet 便可以解决合法的 IP 地址不够用的问题。公司局域网的用户通过代理服务器访问外界时,可以只映射一个 IP 地址,这样公司就不必租用多个 IP 地址了。

### ③ 网址过滤和访问权限限制

代理服务器可以设置 IP 地址过滤功能,对外界或内部的 Internet 地址进行过滤,限制不同用户的访问权限。例如代理服务器可以用来限制封锁 IP 地址,禁止用户浏览某些网页。

### ④ 提高访问速度

代理服务器将远程服务器提供的数据保存在自己的硬盘上,如果有许多用户同时使用这一个代理服务器,当有人访问过某一站点后,所访问站点的内容便会被保存在代理服务器的硬盘上,如果下一次再要访问这个站点时,这些内容便会直接从代理服务器磁盘中取得,而不必再次连接到远程服务器上获取。因此,使用代理服务器可以节约带宽、提高访问速度。

## 2. 代理服务器的工作原理

代理服务器(Proxy Server)的工作原理是:当用户在浏览器中设置好代理服务器后,使用浏览器访问所有 WWW 站点的请求都不会直接发送给目的主机,而是先发送给代理服务器,代理服务器接受了用户的请求以后,向目的主机发出请求,并接受目的主机的数据,存于代理服务器的硬盘中,然后再将用户要求的数据发给用户。

下面来详细说明其工作过程:

当用户端对服务器端提出请求时,此请求会被发送到代理服务器,然后代理服务器会检查本身是否有用户端所需要的数据。如果有而且没有过期,代理服务器便代替服务器将数据传给用户端。而用户端一般会选择距自己传输距离较近的某台代理服务器,所以从代理服务器申请得到数据的速度可能会比从远程服务器申请数据要快。

如果代理服务器没有用户端所请求的数据或数据已经过期,它会去服务器获取所需的数据。在代理服务器从服务器端取得数据传给用户端时,自己保存一份,待下次如果有用户提出相同的请求时,便可以将数据直接传过去,而不需要再去服务器端获取了,如图 3.60 所示。

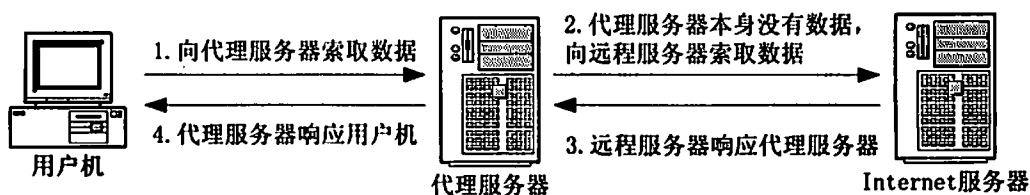


图 3.60 代理服务器工作原理示意图

## 3. 代理服务器的适用环境和对硬件的要求

无论是家庭还是公司,都不可能为每一台计算机都申请或租用一个合法的 IP 地址。要使内部的多个计算机用户高效、安全地访问 Internet,使用代理服务器是一种最好的选择。代理服务器至少需要拥有一个合法的 IP 地址,为内部局域网中的每一台用户机都分配一个独立的 IP 地址,并且通过在用户机软件上配置使用代理服务器(如用 Microsoft Internet Explorer 浏览器设置)、指向代理服务器的 IP 地址和服务端口,从而使局域网内部的众多用户通过代理服务器访问 Internet。

对于局域网内部的用户来说,是利用资源共享,实现局域网内部用户对 Internet 的访问;



而对于服务器来说,一般是使用专线,实现多台计算机同时访问 Internet 的目的。

代理服务器能实现许多功能,它对服务器的硬件有一定要求。通常安装代理服务器软件的计算机需要一个较大的硬盘作为访问数据存放的缓冲区(可能高达几个 GB 或者更大),当接收到远程服务器提供的信息时,就将其保存到缓冲区中,当其他用户再访问相同的信息时,直接由缓冲区取出信息传送给用户,以提高访问速度。因为代理服务器需要保持多路连接,这会使用大量的内存,所以它需要大容量的内存;在一定环境下,有的代理软件需要两个或更多的网卡。

#### 4. 代理服务器的架设

代理服务器在运行方式上可以分为透明代理和传统代理两类。下面介绍的 WinGate 代理服务器既可以作透明代理,也可以作传统代理。但这两种代理方式,用户端的网络设置和软件设置并不相同。下面以一个例子来说明两种代理用户机的设置方式。

假如某公司向 ISP 申请了 ADSL 业务以接入 Internet,相关参数为:IP 地址为 220.102.168.10、子网掩码为 255.255.255.248、默认网关为 220.102.168.10、DNS 为 202.102.192.68。现通过一台代理服务器,实现整个公司用户访问 Internet。

##### (1) 代理服务器的网络设置

① 安装硬件。在代理服务器中安装一块 ADSL 接口卡用于接入 Internet,安装一块网卡用于接入公司内部局域网。

② 设置 ASDL 接口卡网络参数。IP 地址为 220.102.168.10、子网掩码为 255.255.255.248、默认网关为 220.102.168.10、DNS 为 202.102.192.68,如图 3.61 所示。访问 Internet 看是否能正常访问,如能访问,则说明接入 Internet 已经设置好了。

③ 设置网卡的网络参数。假设局域网使用配置 192.168.1.0/24 这个 C 类地址,使用它的第一个 IP 地址(192.168.1.1)作为该网卡的 IP 地址,子网掩码为 255.255.255.0,其他参数可以不设置。

④ 安装代理服务器软件,并进行相关配置。

通过上面 4 个步骤,代理服务器基本设置完毕。

##### (2) 用户机的网络设置

###### ① 透明代理

透明代理的意思是用户端根本不需要知道有代理服务器的存在。用户机好像就直接连接到 Internet 上,用户端需做如下设置:一是设置网络参数,包括 IP 地址(范围 192.168.1.2~192.168.1.254)、默认网关为 192.168.1.1、DNS 为 202.102.192.68,如图 3.61 所示;二是安装用户端软件并做相应设置。

###### ② 传统代理

在传统代理中,用户端网络设置比较简单,只需要设置 IP 地址就可以了,不需要安装用户端软件。在这个例子中,用户端 IP 地址设置范围为 192.168.1.2~192.168.1.254,默认路由、DNS 都可以不设置。但在应用软件上(如 IE、QQ、CuteFTP 等)必须要做相应设置,主要有两个参数:一个是代理服务器的 IP 地址(本例中设为 192.168.1.1),一个是端口号,对于不同服务端口号可能不同。

不论是采用透明代理还是传统代用,客户机的参数都可以通过 DHCP(动态主机分配协

议)来动态分配 IP 地址和相关参数,这样可以简化网络管理。DHCP(动态主机分配协议)将在下一节中介绍。

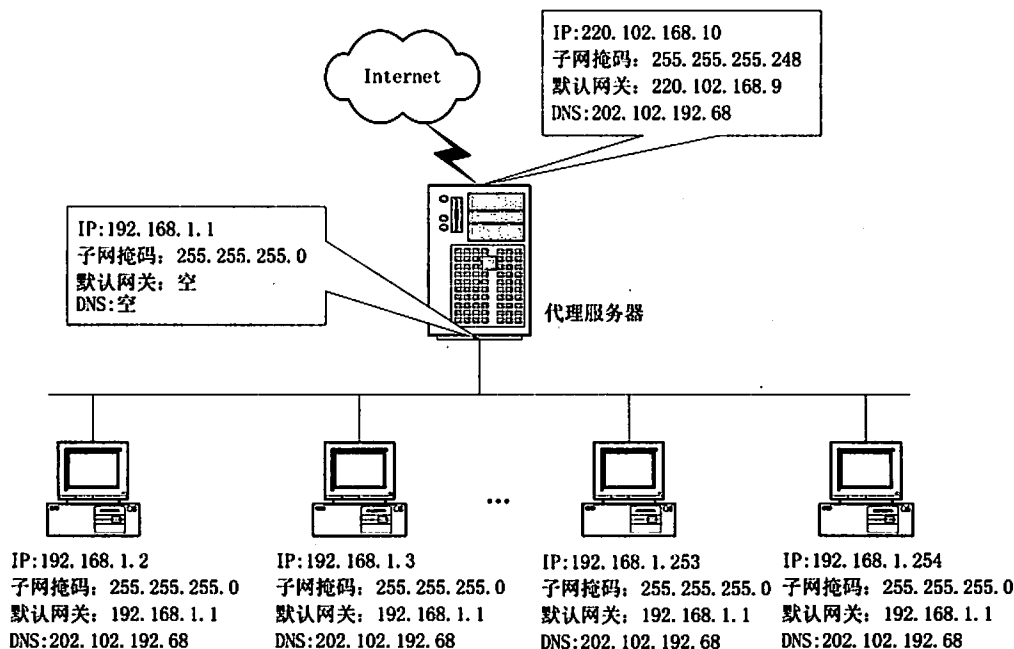


图 3.61 透明代理的网络配置

### 3.6.1.2 WinGate 代理服务器的安装与配置

#### 1. WinGate 服务器端的下载和安装

(1) 下载软件: 到 WinGate 官方网站 [www.wingate.com](http://www.wingate.com) 下载 WinGate 的最新版本, 最新版本是 6.0 版本, 这里只介绍比较稳定的 5.2.3 版本。

(2) 双击 `wgsetup.exe`, 将弹出 WinGate 安装协议书, 单击【I Agree】按钮, 如图 3.62 所示。

(3) 选择安装类型, 选中【Configure this Computer as the WinGate Server】单选按钮, 单击【Continue】按钮, 如图 3.63 所示。弹出对话框提示安装的是 Server 版, 单击【Next】按钮。

(4) 提供几种注册模式供选择, 如无序列号, 则单击【Evaluate winGate Home, standard or Pro(FREE 30 DAY trail)】, 试用 30 天, 如已获得序列号, 则单击【Install WinGate(enter yourWinGate key below)】, 然后在 License Name 与 License key 下的文本框中分别输入用户名与序列号, 输入完毕后单击【Next】按钮, 如图 3.64 所示。

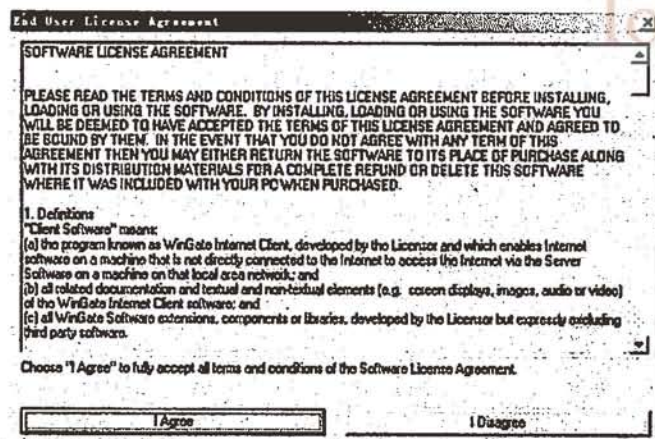


图 3.62 许可协议



图 3.63 选择安装类型

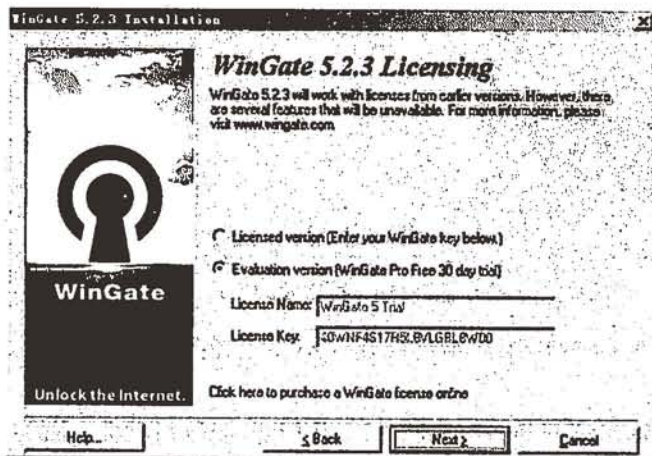


图 3.64 选择注册方法

(5) 出现一些提示信息，单击【Next】按钮继续，然后要求选择路径，WinGate 默认

安装路径是 C:\Program Files\WinGate，单击右边的【...】按钮更改安装路径，一般选择默认安装路径即可，单击【Next】按钮，如图 3.65 所示。

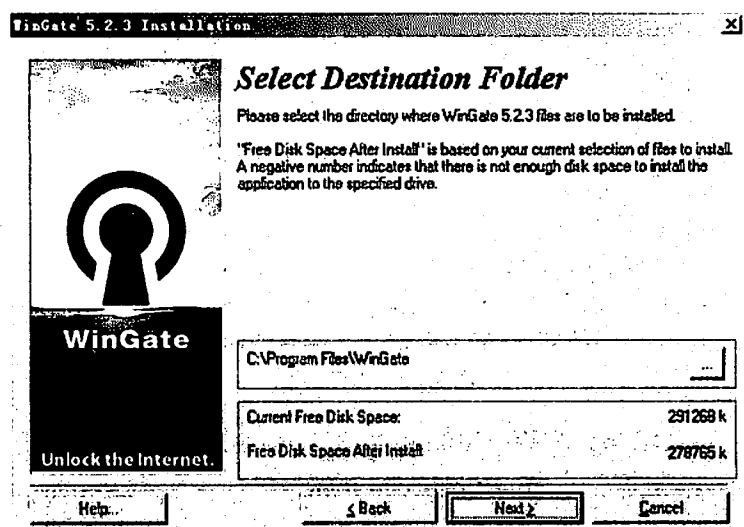


图 3.65 选择安装位置

(6) 弹出对话框，要求选择是典型安装还是自定义安装。选中【Express setup (recommended)】单选按钮，单击【Next】按钮继续，如图 3.66 所示。

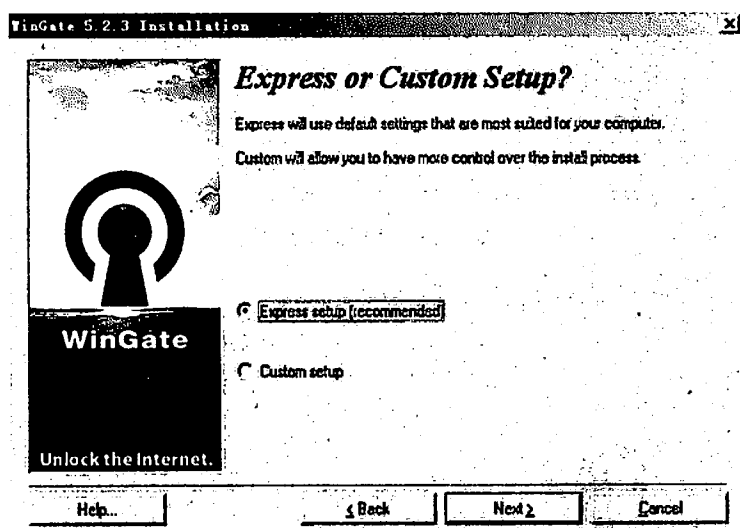


图 3.66 选择安装模式

(7) 询问是否使用 NT 用户验证，建议不要选择此项，单击【Next】按钮继续，如图 3.67 所示。

(8) 出现对话框，询问是否启用软件的 E-Mail 服务器功能，若想启用，输入 E-Mail 服务器域名。建议不选择此项，单击【Next】按钮，如图 3.68 所示。

(9) 弹出的对话框询问是否安装扩展网络支持功能，如需安装扩展网络支持功能，则选择 Install ENS 选项。建议不选择此项，单击【Next】按钮，如图 3.69 所示。



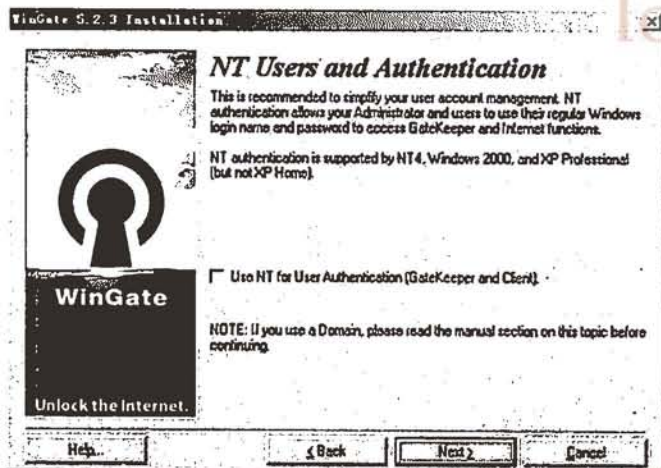


图 3.67 选择用户验证方式

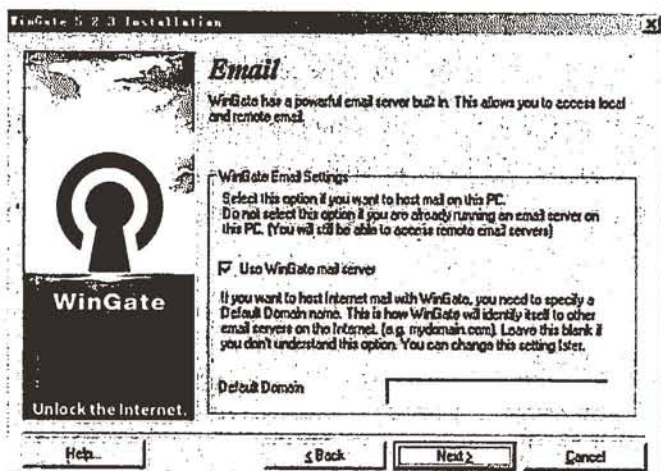


图 3.68 是否启用 E-Mail 服务器

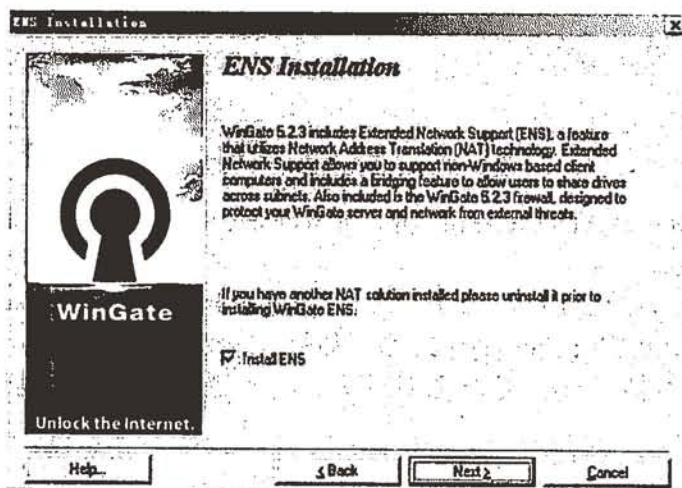


图 3.69 是否安装扩展网络支持功能

(10) 弹出的对话框询问是否安装 VPN, 如需安装 VPN, 则选择【Install VPN】选项。建议不选择此项, 单击【Next】按钮, 如图 3.70 所示。

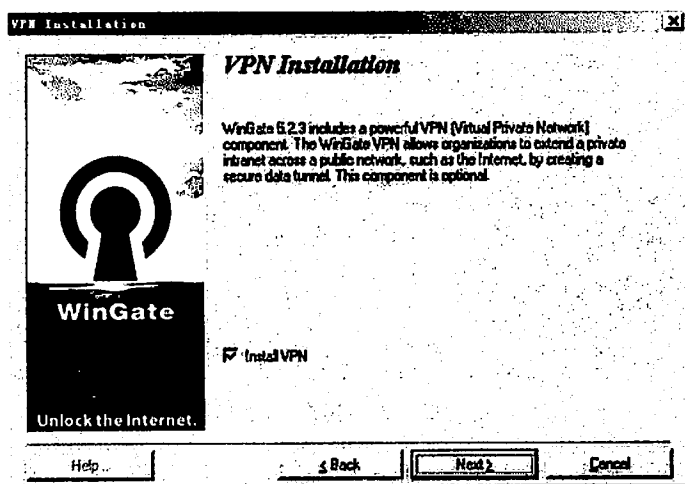


图 3.70 是否安装 VPN

(11) 弹出的对话框询问是否自动升级 WinGate, 如需自动升级, 则选择【Enable Auto Update】选项, 单击【Next】按钮继续, 如图 3.71 所示。

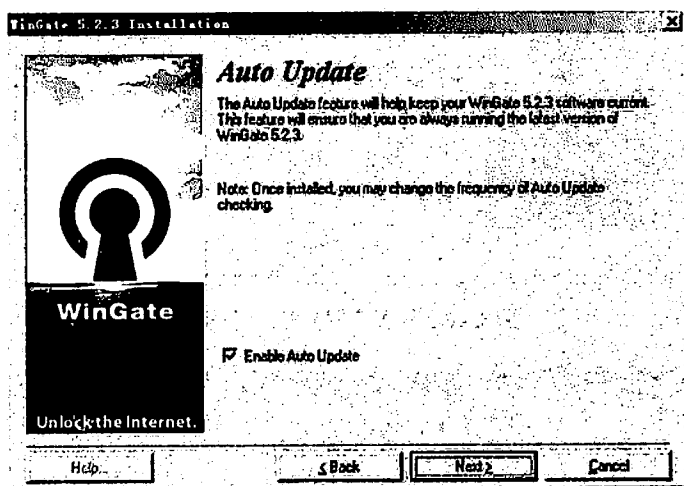


图 3.71 是否支持自动升级功能

(12) 弹出开始安装 WinGate 界面, 并显示 WinGate 的安装路径, 单击【Begin】按钮继续, 如图 3.72 所示。

(13) WinGate 开始复制文件, 复制完成后, 并显示 Installation Completed 对话框, 单击【Finish】按钮即可完成 WinGate 的安装, 如图 3.73 所示。

WinGate 安装完成后, 提示是否重启计算机, 选择“是”即可。重新启动计算机后 WinGate 将自动启动。

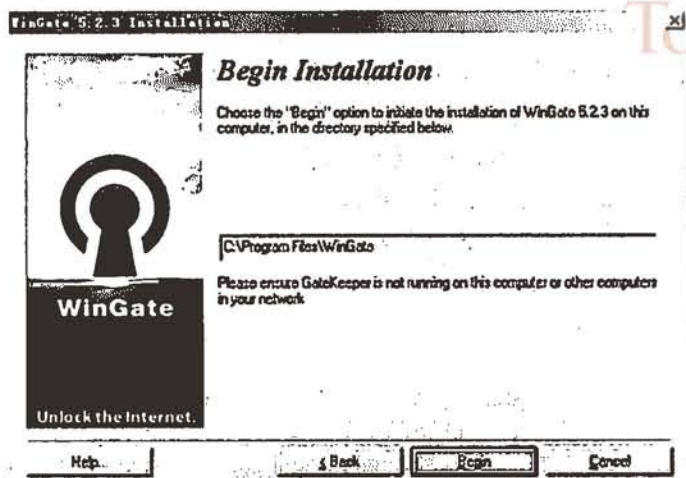


图 3.72 是否开始安装

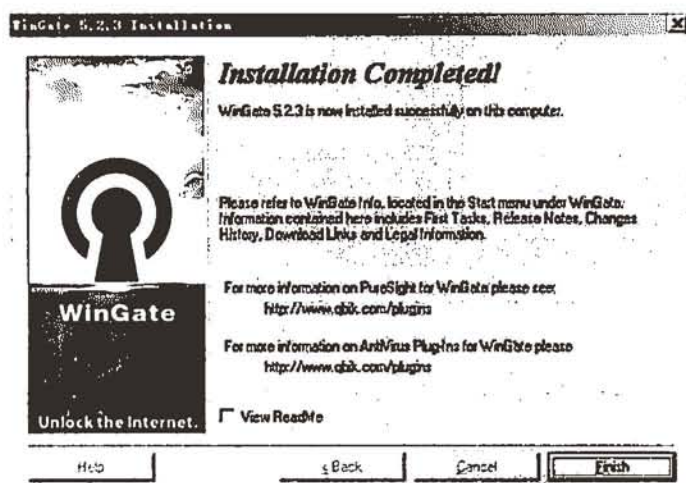



图 3.73 完成安装

## 2. WinGate 服务器端的基本设置

(1) 设置 WinGate 管理员密码。WinGate 安装成功后，每次启动计算机都会自动运行，并在任务栏生成一个 WinGate 的图标  0:22，双击该图标，要求输入 WinGate 管理员的密码，由于刚安装 WinGate，未设置密码，单击 OK 按钮即可，如图 3.74 所示。然后 WinGate 弹出对话框，提示为了系统的安全，必须要设置密码，单击 OK 按钮，弹出【Set Administrator Password】对话框，在【New Password】和【Confirm New】处输入相同的密码，单击 OK 按钮。

(2) 认识 WinGate 管理主界面。双击任务栏的 WinGate 图标，输入刚才设置的管理员密码，进入 WinGate 的管理主界面，如图 3.75 所示。WinGate 管理主界面主要分两大块，左边的为系统设置，右边为消息显示。System 系统选项卡主要

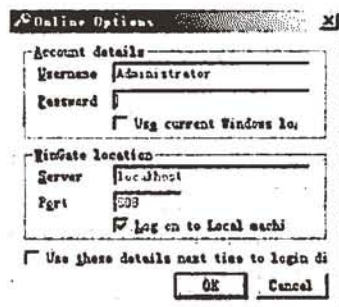


图 3.74 服务器登录对话框

用来设置 WinGate 的核心服务, 如 DHCP 服务、DNS 服务、Caching 的设置、DNS 扩展网络支持的管理等等, 一般来说, WinGate 的默认设置就已经可以很好地工作了, 无须做太多的修改。Services 服务选项卡用于设置 WinGate 代理服务的核心, 如 WWW 服务, Socks 服务, SMTP、POP3 服务等。Users 用户选项卡用于添加设置用户权限、用户组等。Activity 选项卡用于显示 WinGate 的运行状态。History 选项卡用于记录用户最近访问过的网站。System Messages 选项卡用于对 WinGate 系统信息的管理。由于 system、Services 的各项服务基本上可采取 WinGate 的默认设置值, 这里主要是对账户进行管理。

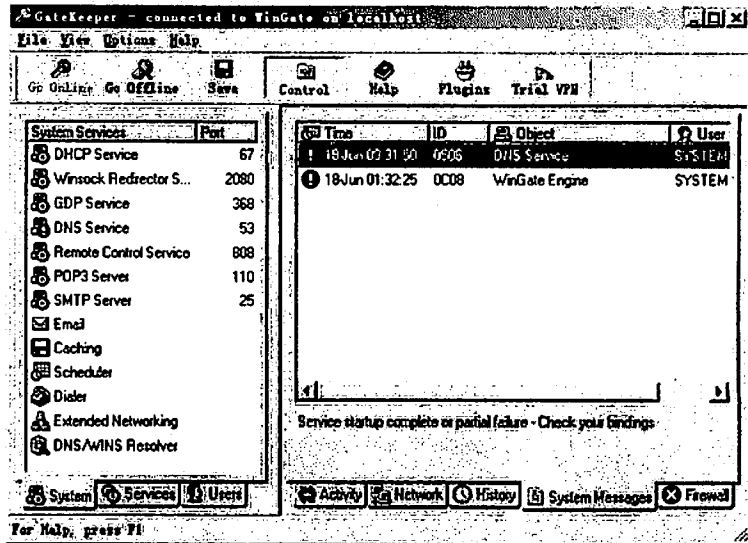


图 3.75 WinGate 的管理主界面

(3) 新建账户。WinGate 对各台客户端进行管理, 实际上大部分是通过对账户进行管理实现的, 以新建“zhang”账户为例, 介绍怎样新建一个账户。具体操作步骤为: 进入 WinGate 管理主界面, 单击 users 选项卡, 右击 Users, 在弹出的快捷菜单中选中 New User, 弹出 Properties for new users 对话框, 如图 3.76 所示。在 Properties for new users 对话框中, 选择 User Info 选项卡, 在 user name 文本框中输入“zhang”, 在 Real name 文本框中输入“zhang wurong”, 在 Password 和 confirm 文本框中输入相同的密码, 单击 OK 按钮即可。

(4) 新建用户组。组就是将多个账户统一管理, 赋予其相同的权限, 以新建“teachers”组为例, 并将“zhang”、“tao”两个账户添加至该组, 介绍怎样创建一个用户组, 并将账户添加到组。操作步骤: 右击 Groups, 在弹出的快捷菜单中选择 New Groups, 弹出 New Group 对话框, 如图 3.77 所示; 在 Group Name 的文本框中输入组名“teachers”, 然后在 Non-Members 列表中选择“zhang”、“tao”, 单击 Add 按钮, 将这些用户添加到该组。

(5) 指定用户名与计算机的对应关系。创建用户与组后, 需要将用户与计算机建立对应关系, 才能更好地进行管理, 这里将以“zhang”与 IP 地址为 192.168.10.168 的计算机建立相对应的关系为例进行介绍。操作步骤: 在 WinGate 管理主界面, 选择 Users 选项卡, 然后双击 Assumed Users, 弹出 Assumed Users 对话框, 如图 3.78 所示; 用户与计算机建立对应关系, 可以与计算机名或计算机的 IP 地址建立对应关系, 为方便管理, 一般是与 IP 地址建立相对应的关系; 单击 Add 按钮, 弹出对话框, 在 if a user connects from IP address



的文本框中输入与之对应的 IP 地址 192.168.10.168, 在 Then assume it 下拉列表框中选择“zhang”, 单击 OK 按钮; 用同样的方法将“tao”分别与 192.168.10.188 建立对应关系, 单击 OK 按钮。



图 3.76 新建账户

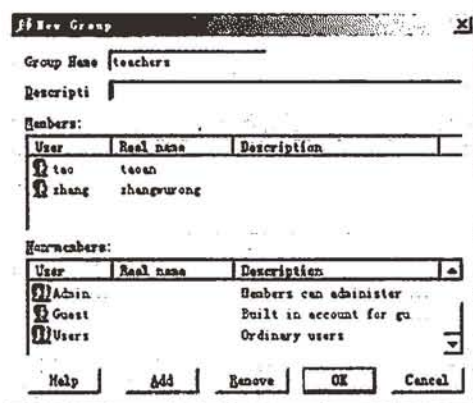


图 3.77 新建用户组

(6) 限制只有注册用户才能访问 Internet。WinGate 的默认状态是启用 guest 账户, 客户端无须登录, 只需设好代理地址, 即可通过 WinGate 代理上网, 如何限制只有授权用户才能访问 Internet 呢? 操作步骤如下: 进入 WinGate 管理主界面, 选择 Users 选项卡。双击 System Policies, 弹出 System Policies 对话框, 如图 3.79 所示; 在弹出的窗口中双击“Everyone”用户, 在弹出的对话框中单击 Recipient 选项卡, 选中 User may be assumed 单选按钮。单击 OK 按钮即可。

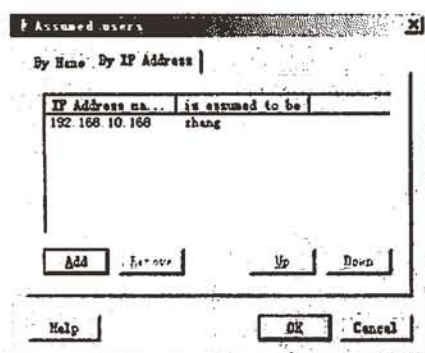


图 3.78 用户名与计算机的对应

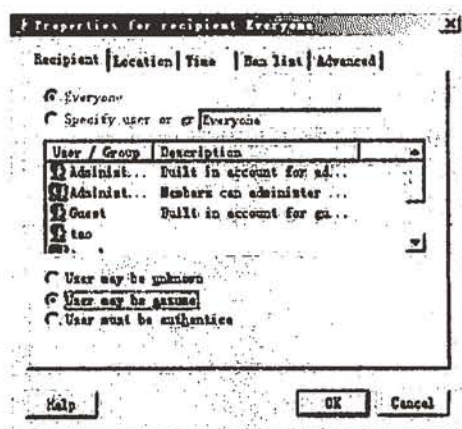


图 3.79 限制非注册用户的访问

(7) 限制访问网站。在管理 WinGate 的过程中, 有时需要对网站的内容进行过滤, 有不良信息则禁止访问。WinGate 默认设置没有任何限制, 要实现这些功能, 需要对设置进行修改, 具体操作步骤如下: 进入 WinGate 管理主界面, 选择 Services 选项卡, 双击 WWW Proxy server, 弹出 WWW Proxy server properties 对话框, 如图 3.80 所示, 选择 Policies 选项卡, 将 Default rights 的选项改为“are ignored”, 表示非窗口列中允许的用户权限均不能访问; 单击 Add 按钮, 弹出 Properties for new recipient 对话框, 然后选择 Ban list 选项卡;

单击 Add 按钮, 弹出 Criterion 对话框, 这个对话框其实就是一个规则表达式, 数据来源可以为服务器域名、服务器 IP 和服务器 URL, 规则表达式可以是等于或包含某些特定字符串, 或以特定的字符串开始或结尾。把来源设为“HTTP URL”, 规则设为“contains(包含)”, 限制字符串输入“sex”, 则表示不准当前用户访问包含有“sex”的网站, 单击 OK 按钮, 如图 3.81 所示; 重复上一步, 将需要禁止访问的两站添加进来, 可以是关键字, 也可以是网站的 URL 全称。

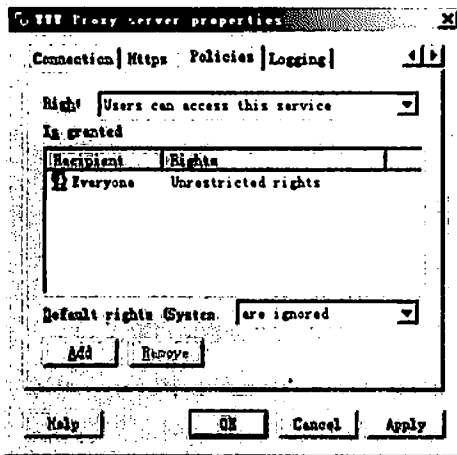


图 3.80 禁止访问包含“sex”的 URL

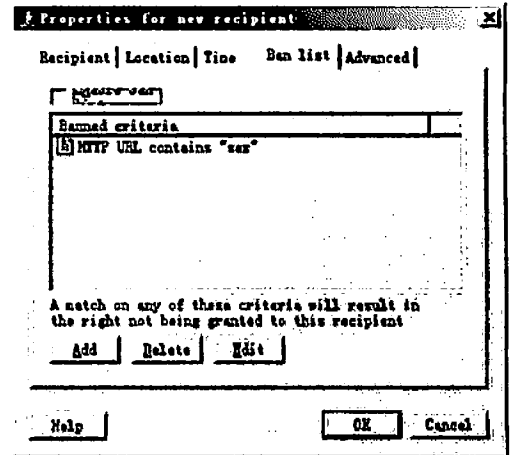


图 3.81 禁止访问包含“sex”的 URL

(8) 限制下载文件。有时为了节省带宽, 不希望客户端下载文件, WinGate 为我们提供了禁用下载文件的方法, 具体操作步骤如下: 进入 WinGate 管理主界面, 选择 Services 选项卡, 双击 WWW Proxy server, 弹出 WWW Proxy server properties 对话框; 选择 Policies 选项卡。将 Default right 的选项改为“are ignored”, 表示非窗口列中允许的用户权限均不能访问; 单击 Add 按钮, 弹出 Properties for new recipient 对话框, 然后选择 Ban list 选项卡; 单击 Add 按钮, 弹出 Criterion 对话框, 如图 3.82 所示, 将表达式改为“HTTP URL”、“ends with”、“zip”即可, 这表示不准用户下载以.zip 为扩展名的文件; 重复上一步也可以将 rar、.exe、.cab、.iso、.img 等文件进行限制下载。

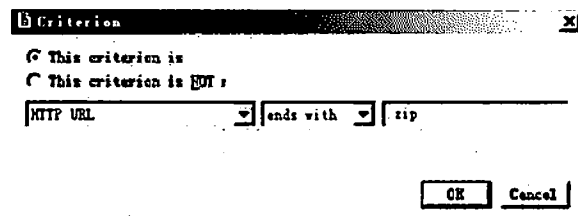


图 3.82 禁止下载以.zip 为扩展名的文件

(9) 指定浏览时间。操作步骤是: 进入 WinGate 管理主界面, 选择 Services 选项卡, 双击 WWW Proxy server, 弹出 WWW Proxy server properties 对话框; 选择 Policies 选项卡, 将 Default right 的选项改为 are ignored, 表示非窗口列中允许的用户权限均不能访问; 单击 Add 按钮, 弹出 Properties for new recipient 对话框, 然后选择 Time 选项卡; 单击 Specify times when this recipient has right 选项按钮, 可以看到 Time 选项卡下有 Included times 和 Excluded



time 列表框, Included times 列表框是设置允许使用时间段, 系统到时会自动开启服务, 而 Excluded time 列表框则是设置拒绝使用时间段, 到时会自动关闭服务。设置拒绝时间段, 单击 Excluded time 列表框的 Add 按钮, 弹出 Time Slice 窗口, 如图 3.83 所示, 在该窗口设置拒绝时间段, 单击 OK 按钮。使用同样方法, 可设置允许使用时间段。

(10) 禁用 WinGate 的 DHCP 功能。有时候客户端自动获取的 IP 地址与 Windows 2000 服务器所设置的不一样(这里包括网关、DNS 等信息), 但进入 Windows 2000 的 DHCP 服务下查看却未查出是什么问题。其实问题所在是启用了 WinGate 的 DHCP 服务, 同一子网有两个 DHCP 服务器, 造成相互之间争抢资源的现象。解决的方法是禁用 WinGate 的 DHCP 功能, 具体操作方法是: 进入 WinGate 管理主界面, 选择 System 选项卡, 双击 DHCP Service, 弹出的窗口如图 3.84 所示, 选择 General 选项卡, 在该选项卡的 Start options 子选项的 Service 的下拉列表中选择 Service is disabled, 禁止使用 DHCP 服务, 单击 OK 按钮。

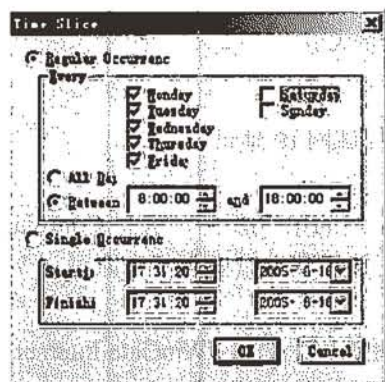


图 3.83 指定浏览时间



图 3.84 禁用 WinGate 的 DHCP 功能

(11) 设置缓存的大小。WinGate 可以对网页文件及其他文件进行缓存。缓存的大小需要合理配置, 缓存过小会影响访问速度, 过大则会对系统的稳定性产生影响。WinGate 默认缓存大小为 200MB, 一般设置成 100~150MB 比较合适。修改缓存的具体操作步骤如下: 进入 WinGate 管理主界面, 单击 Services 选项卡, 单击 Caching 按钮, 弹出 Cache Properties 对话框, 如图 3.85 所示, 在 Limit cache size 文本框中, 将 200 修改为 150, 单位是 MB, 将 Number of days before rechecking HTML files 改为 2, Number of days before rechecking other files 修改为 10。

### 3. 配置 WinGate 客户端

WinGate 既可工作在透明代理方式之下, 也可工作在传统代理方式之下。因此, 客户端使用 WinGate 服务器有两种配置方法: 一种是安装 WinGate 客户端软件(透明代理方式); 另一种是直接对各个客户应用进行设置(传统代理方式)。下面分别作这两种代理方式:

#### (1) 透明代理方式

这要求在每一台客户机上安装 WinGate 客户端软件, 这样客户端软件会自动搜寻到 WinGate 服务器, 所有客户端网络应用均不需作任何设置, 就像直接连接到网络上一样方

便。其操作步骤如下:

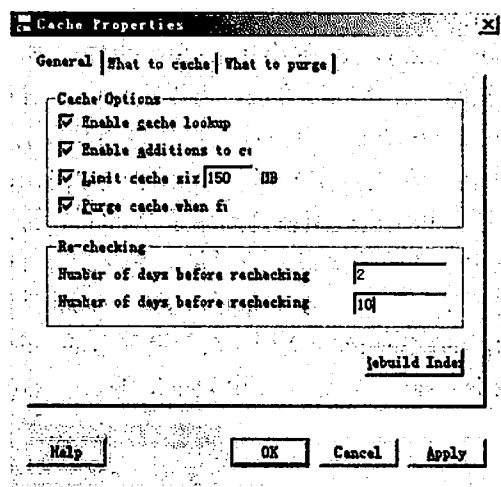


图 3.85 设置 WinGate 缓存的大小

#### ① 设置网关

要将此客户机的网关设成 WinGate 服务器的内部局域网 IP 地址。

#### ② 安装 WinGate 客户端软件

WinGate 客户端软件和服务器安装相似,只是在上述的第(3)步中,选择 Configure this Computer as a WinGate Internet Client,然后同上面的安装步骤继续安装下去即可。

#### ③ WinGate 客户端软件的安装

在 WinGate 客户端软件安装完后,只要打开【开始】|【程序】|WinGate Internet Client | WinGate Internet Client Applet 文件,在 General(常规)选项卡中选中 Enable the WinGate Internet Client,如图 3.86 所示,即可激活客户端,其他可不需作设置。

#### (2) 传统代理方式

传统代理方式,这种方法的好处是不需要安装客户端软件,在客户端应用软件上直接进行设置即可访问 Internet。

下面是一些常用客户端应用软件的设置。

##### ① Microsoft Internet Explore (IE)

打开【控制面板】|Internet【连接】|【局域网设置】在弹出的对话框中设置。打开【使用代理服务器】复选框,在【地址】中填写 WinGate 服务器的内部局域网 IP 地址,端口中填入“80”,并单击【确定】按钮。如果要具体进行设置,可单击【高级】选项卡,即可对服务进行设置,如图 3.87 所示。

##### ② Netscape

选择 Netscape 后,在菜单中选择 Edit | Preferences 命令,在 Netscape 系统设置对话框中选择 Advanced | Proxies,选中 Manual Proxy Configuration 单选按钮,单击 View 按钮后将弹出手工设置代理服务器对话框,如图 3.88 所示。在弹出的对话框中填入如下内容:

HTTP: WinGate 服务器的内部局域网 IP 地址, PORT 为 80;

FTP: WinGate 服务器的内部局域网 IP 地址, PORT 为 21;



SOCKS: WinGate 服务器的内部局域网 IP 地址, PORT 为 1080。

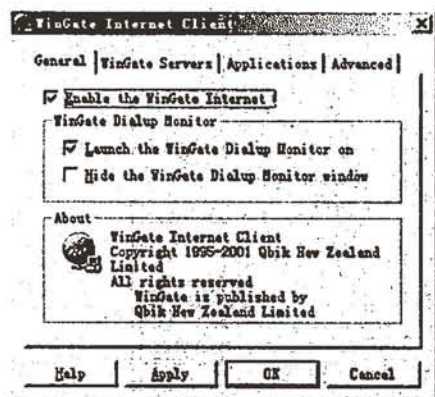


图 3.86 WinGate 客户端软件的设置

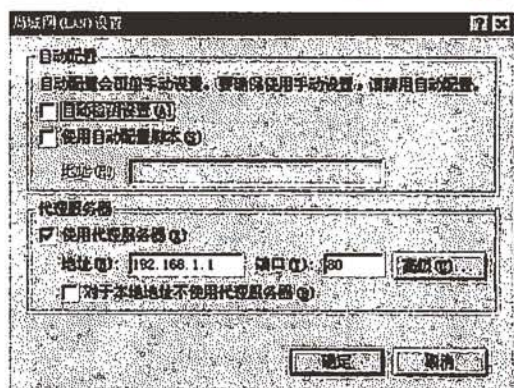


图 3.87 IE 浏览器代理服务器设置

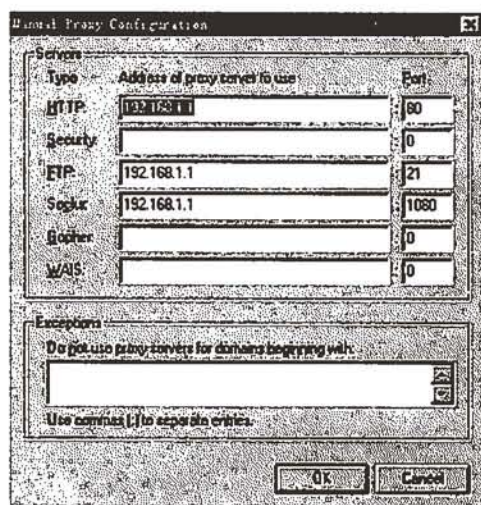


图 3.88 Netscape 浏览器代理服务器设置

### ③ CuteFTP

打开 CuteFTP 后在主菜单中选择 Edit | Settings, 然后在弹出的对话框中选择 Connection | Socks 目录进行设置, 如图 3.89 所示。

在图 3.89 中, 选择 Socks 5 单选按钮, 在 Host 文本框中填写 WinGate 服务器的内部局域网 IP 地址; Port 文本框中填写 1080, 最后单击 OK 按钮。

### ④ 电子邮件客户端的设置(Outlook Express)

在 POP3 和 SMTP 的地址都填写 WinGate 服务器的内部局域网 IP 地址, 在账号或用户名中填入“账号名#邮件服务器名”(注意用“#”号)。例如在 www.tom.com 中申请了一个地址为 testuser@tom.com 的邮箱, 那么账号名中应填写“testuser#tom.com”, 其他设置都一样, 如图 3.90 所示。

### ⑤ 腾讯 QQ 2004

打开腾讯 QQ 2004 后, 在用户登录对话框中, 单击【网络设置】按钮, 在【类型】中

选择【Socks 5 代理】，在地址中输入 WinGate 服务器的内部局域网 IP 地址，端号为 1080，单击【测试】按钮看代理服务器工作是否正常，如果正常，即可按正常程序输入 QQ 号码和密码就可使用了，如图 3.91 所示。

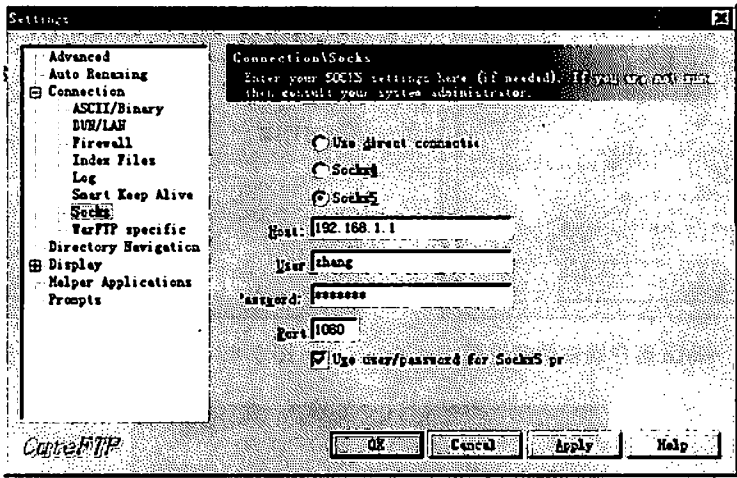


图 3.89 CuteFTP 浏览器代理服务器设置

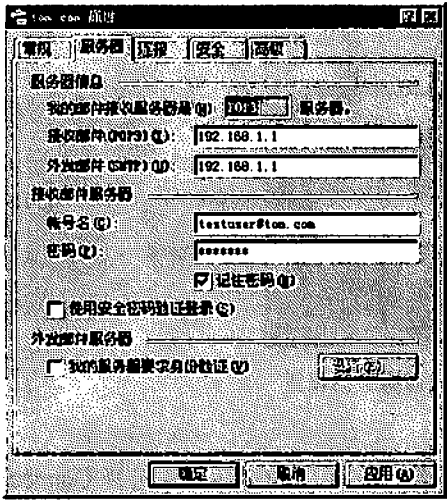


图 3.90 Outlook Express 代理服务器设置



图 3.91 QQ 2004 代理服务器设置

⑥ NetAnts

打开 NetAnts 后选择【选项】|【参数设置】|【代理】对话框在出现的代理对话框中输入：名称可任意填写，如填入 testptoxy，类型选择 SOCKS 5，地址输入 WinGate 服务器的内部局域网 IP 地址 192.168.10.10，端号为 1080，如图 3.92 所示。

⑦ telnet

打开【开始】|【运行】对话框，在【运行】对话框中输入“telnet <WinGate 服务器的内部局域网 IP 地址>”，然后会出现列选框，然后再输入所要 telnet 的地址或域名即可。

### ⑧ RealPlayer

安装好 RealPlayer，选择【控制面板】| RealPlayer 对话框，在打开的对话框中选择【代理服务器】选项卡，然后选择【手工配置 HTTP 代理服务器】单选按钮，并将下列文本框【代理服务器】处输入 WinGate 服务器的内部局域网 IP 地址，【端口】处输入 80，如图 3.93 所示。

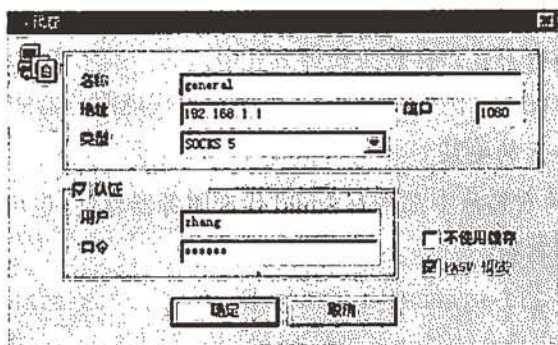


图 3.92 NetAnts 代理服务器设置

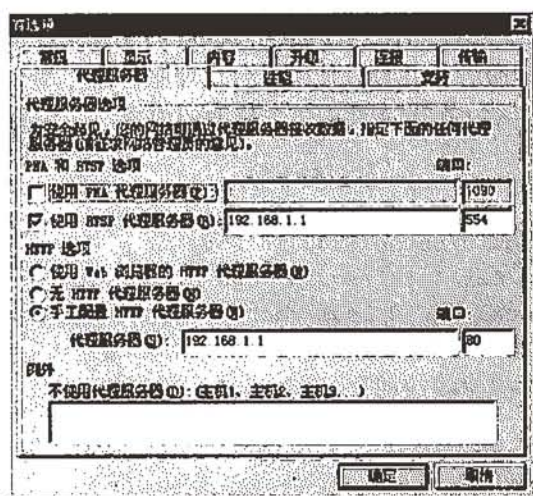


图 3.93 RealPlayer 代理服务器设置

### 3.6.1.3 Linux 下 Squid 代理服务器配置与管理

Linux 环境下的代理服务器的软件较多，但实践证明被广泛应用的高性能代理服务器只有少数几个，Squid 就是其中之一。

对于 Web 用户来说，Squid 是一个高性能的代理缓存服务器，它支持 HTTP、FTP 和 GOPHER 协议。与一般代理缓存软件不同，Squid 用一个单独的、非模块化的、I/O 驱动的进程来处理所有客户端的请求。

Squid 将数据源缓存在内存中，同时也缓存 DNS 的查询结果。除此之外，它还支持非模块化 DNS 查询，对失败的请求进行消极缓存。Squid 支持 SSL 协议，支持访问控制。由于使用了 ICP(轻量级 Internet 缓存协议)，Squid 能够实现层迭的代理阵列，从而最大限度



的节省带宽。

Squid 由一个主要服务程序 Squid、一个 DNS 查询程序 dnsserver、几个重写请求和执行认证的程序,以及几个管理工具组成。当 Squid 启动后,它可派生出预先指定数目的 dnsserver 进程,而每一个 dnsserver 进程都可单独进行 DNS 查询,从而大大减少了服务器等待 DNS 查询的时间。

Squid 的代理方式既可以是传统代理,也可以是透明代理,由于透明代理比较复杂,这里只介绍传统代理的运行方式。在传统代理方式中,客户端不需要安装客户端软件,但需要对应用软件做相应的设置。例如在 IE 中,需要设置代理服务器的地址和代理端口号。

### 1. Squid 代理服务器的安装

在 Red Hat Linux 的安装盘中都带有 Squid 代理服务器软件,也可以在网上下载安装包。执行如下命令即可完成安装:

```
#rpm -ivh squid-2.3-STABLE4-1.i386.rpm      //2.3-STABLE4-1 为 Squid 版本号
```

### 2. Squid 代理服务器的配置

Squid 有一个主要配置文件 /etc/squid/squid.conf, 该配置文件很长, 默认的 /etc/squid/squid.conf 长达到 2177 行之多。虽然 Squid 的配置文件很庞大, 但是若用户只是一个中小型网络提供代理服务, 并且只使用一台代理服务器, 那么只需要修改配置文件中的几个选项即可。下面列举了配置文件中需要修改的内容, 并作简要介绍。

```
http_port 8080
cache_mem 32 MB
cache_dir /home/squid/cache 1200 16 256
cache_access_log /usr/local/squid/logs/access.log
cache_log /usr/local/squid/logs/cache.log
dns_nameservers 210.12.114.130
acl all src 0.0.0.0/0.0.0.0
http_access allow all
cache_mgr jim@abc.com.cn
```

#### (1) http\_port

该选项用于定义 Squid 监听 HTTP 客户连接请求的端口。默认值是 3128, 如果使用 HTTPD 加速模式则为 80。可以指定多个端口, 但是所有指定的端口都必须在一条命令行上。例如:

```
http_port 8080      #表示代理服务器监听的端口为 8080。
```

#### (2) cache\_mem

该选项用于指定 Squid 可以使用的内存的理想值, 单位为 bytes。

#### (3) cache\_dir

该选项用于指定 Squid 用来存储对象的交换空间的大小及其目录结构。

```
cache_dir <目录> <大小> <一级目录数> <二级目录数>
```

可以用多个 cache\_dir 命令来定义多个这样的交换空间, 并且这些交换空间可以分布不



同的磁盘分区。“目录”(directory)指明了该交换空间的顶级目录。“大小”定义了可用的空间总量，其单位是 Mbytes。需要注意的是，Squid 进程必须拥有对该目录的读写权力。

“Level-1”是可以在该顶级目录下建立的第一级子目录的数目，默认值为 16。同理，“Level-2”是可以建立的第二级子目录的数目，默认值为 256。为什么要定义这么多子目录呢？这是因为如果子目录太少，则存储在一个子目录下的文件数目将大大增加，这也会导致系统寻找某一个文件的时间大大增加，从而使系统的整体性能急剧降低。所以，为了减少每个目录下的文件数量，我们必须增加所使用的目录的数量。如果仅仅使用一级子目录则顶级目录下的子目录数目太大了，所以我们使用两级子目录结构。

那么，怎么来确定你的系统所需要的子目录数目呢？我们可以用下面的公式来估算。

已知量：

DS = 可用交换空间总量(单位 KB)/交换空间数目

OS = 平均每个对象的大小= 20KB

NO = 平均每个二级子目录所存储的对象数目= 256KB 单位

未知量：

L1 = 一级子目录的数量

L2 = 二级子目录的数量

计算公式：

$L1 \times L2 = DS / OS / NO$

注意这是个不定方程，可以有多个解。

如果不想 Squid 缓存任何文件，如某些存储空间有限的专有系统，可以使用 null 文件系统(这样不需要那些缓存策略)：

```
cache_dir null /tmp
```

#### (4) cache\_access\_log

说明：指定客户请求记录日志的完整路径(包括文件的名称及所在的目录)，该请求可以是来自一般用户的 Http 请求或来自邻居的 ICP 请求。默认值为：

```
cache_access_log /var/log/squid/access.log
```

如果你不需要该日志，可以用以下语句取消：

```
cache_access_log none
```

#### (5) cache\_log

说明：指定 Squid 一般信息日志的完整路径(包括文件的名称及所在的目录)。默认路径为：

```
cache_log /var/log/squid/cache.log
```

#### (6) dns\_nameservers

该选项用来定义 Squid 进行域名解析时使用的域名服务器的，因为在使用代理协议时，客户端并不进行域名查询，而是通过代理进行的，因此需要为代理服务器指定域名服务器来进行域名解析。例如：

```
dns_nameservers 210.12.114.130
```

### (7) acl

说明：定义访问控制列表。定义语法为：

```
acl aclname acltype string1 ...  
acl aclname acltype "file" ...
```

当使用文件时，该文件的格式为每行包含一个条目。

acl type 可以是 src、dst、srcdomain、dstdomain、url\_pattern、urlpath\_pattern、time、port、proto、method、browser、user 中的一种。

分别说明如下：

- src 指明源地址。可以用以下的方法指定：

```
acl aclname src ip-address/netmask ... (客户 IP 地址)  
acl aclname src addr1-addr2/netmask ... (地址范围)
```

- dst 指明目标地址。语法为：

```
acl aclname dst ip-address/netmask ... (即客户请求的服务器的 IP 地址)
```

- srcdomain 指明客户所属的域。语法为：

```
acl aclname srcdomain foo.com ... squid() 将根据客户 IP 反向查询 DNS()
```

- dstdomain 指明请求服务器所属的域。语法为：

```
acl aclname dstdomain foo.com ... () 由客户请求的 URL 决定()
```

注意，如果用户使用服务器 IP 而非完整的域名时，Squid 将进行反向的 DNS 解析来确定其完整域名，如果失败就记录为“none”。

- time 指明访问时间。语法如下：

```
acl aclname time [day-abbrevs] [h1:m1-h2:m2]
```

day-abbrevs: S – Sunday、M – Monday、T – Tuesday、W – Wednesday、H – Thursday、F – Friday、A – Saturday。h1:m1 必须小于 h2:m2，表达式为[hh:mm-hh:mm]。

- port 指定访问端口。可以指定多个端口，比如：

```
acl aclname port 80 70 21 ...  
acl aclname port 0-1024 ... (指定一个端口范围)
```

- proto 指定使用协议。可以指定多个协议：

```
acl aclname proto HTTP FTP ...
```

- method 指定请求方法。比如：

```
acl aclname method GET POST ...
```

这里定义了一个名为 all 的组，包括所有的主机。

#### (8) http\_access

说明：根据访问控制列表允许或禁止某一类用户访问。如果某个访问没有相符合的项目，则默认为应用最后一条项目的“非”。比如最后一条为允许，则默认就是禁止。所以，通常应该把最后的条目设为“deny all”或“allow all”来避免安全性隐患。

#### (9) cache\_mgr

说明：服务器管理者的电子邮件，当发生错误时，该地址会显示在错误页面上，便于用户联系。

### 3. 测试及管理方法

#### (1) 重新启动 Squid 服务

当修改完配置文件后，需要重新启动才能使得 Squid 配置生效。其命令是：

```
#/etc/rc.d/init.d/squid restart
```

#### (2) 初始化 Squid Cache 目录

在为 Squid 初始化 Cache 目录之前，先要更改这个目录的权限，其命令如下：

```
#chmod 0777 /home/squid/cache  
#squid -z
```

#### (3) 测试

在客户端的 IE 浏览器中需要设置代理服务器 IP 地址和端口号，端口号由 http\_port 选项指定。

## 3.6.2 典型例题分析

例 1 代理服务器可以提供 (1) 功能。(2004 年下半年网络管理员上午试题 48)

(1) A. 信息转发 B. 路由选择 C. 域名解析 D. 帧封装

分析：该题主要考查考生对代理的服务器的概念的掌握情况。

代理服务器(Proxy Server)是个人网络和 Internet 服务商之间的中间代理机构，它负责转发合法的网络信息，对转发进行控制和登记。当代理服务器客户端发出一个对外的资源访问请求，该请求先被代理服务器识别并由代理服务器代为向外请求资源，代理服务器再把获得的外部资源转发给代理服务器的客户端。因此代理服务器的最主要的功能是信息转发，即选项 A。另外，选项 B 路由选择一般由路由器来完成的，选项 C 域名解析通常由域名服务器(DNS 服务器)来完成的，选项 D 帧封装是由数据链路层所完成的，尽管代理服务器在进行信息转发时，也需要完成这三个工作，但都不是代理服务器最主要功能。

答案：(1)A

例 2 阅读以下说明，回答问题 1~5，将答案填入对应的答案栏内。

#### 【说明】

某一小型公司已经建成了一个局域网，内部计算机的 IP 地址为 192.168.10.2~192.168.10.254，子网掩码为 255.255.255.0，DNS 和默认网关都没有设置。该公司在 ISP 申请了 Internet 接入，接入方式是以太网，ISP 分配给了一个固定的 IP 地址为 222.152.199.33、

子网掩码为 255.255.255.252、默认网关为 222.152.199.34、DNS 为 202.102.192.68。该公司准备购买一台 PC 服务器作为代理服务器以实现整个公司上网,代理软件准备采用 WinGate 5.0。

**【问题 1】**代理服务器硬件上有什么要求?

**【问题 2】**代理服务器网络配置如何设置?

**【问题 3】**若采用透明代理方式,则客户机如何设置?需要安装何种软件并作何种设置?

**【问题 4】**为了节省带宽,公司不希望员工下载软件,如何设置?

**【问题 5】**为了防止公司在非工作时间上网,如何设置?

**分析:**该题主要考查基于 WinGate 代理服务器的规划和管理。

**问题 1:**代理服务器能实现许多功能,它对服务器的硬件有一定要求。代理服务器都需要一个较大的硬盘作为访问数据存放的缓冲区(可能高达几个 GB 或者更大),当有远程服务器提供的信息通过时,就将其保存到缓冲区中,当其他用户再访问相同的信息时,直接由缓冲区取出信息传送给用户,以提高访问速度,因为代理服务器需要保持多路链接,这会使用大量的内存,所以它需要一个大容量的内存;根据题中的要求,这台代理服务器还必须安装两块网卡。

**问题 2:**在本例中,代理服务器位于 Internet 和内部局域网之间,起桥梁作用,因此连接 Internet 的网卡必须设置 Internet 地址和相关参数,以便代理服务器可以访问 Internet;内部必须设置为局域网内部地址,以便内部客户机能够访问该代理服务器。于是连接 Internet 的网卡必须设置为:IP 地址为 222.152.199.33、子网掩码为 255.255.255.252、默认网关为 222.152.199.34、DNS 为 202.102.192.68;接入内部局域网的设置为:IP 地址为 192.168.10.1,其他参数可以不设置。

**问题 3:**透明代理的意思是客户端根本不需要知道有代理服务器的存在。客户机就直接连接到 Internet 上,客户端需做如下设置:一是设置网络参数,包括 IP 地址、默认网关(代理服务器内网地址)、DNS(和代理服务器的 DNS 一样);二是安装客户端软件并做相应的设置。

**问题 4:**在 WinGate 代理服务器中,管理员可限制客户机对文件的下载。设置方法是:进入 WinGate 管理主界面,单击 Services 选项卡,双击 WWW Proxy server,弹出 WWW Proxy server properties 对话框;单击 Policies 选项卡。将 Default right 的选项改为“are ignored”,表示非窗口列中允许的用户权限均不能访问;单击 ADD 按钮,弹出 Properties for new recipient 对话框,然后单击 Ban list 选项卡;单击 Add 按钮,弹出 Criterion 对话框,将表达式改为“HTTP URL”、“ends With”、“zip”即可,这表示不准用户下载以.zip 为扩展名的文件;重复上一步也可以将.rar、.exe、.cab、.iso、.img 等文件进行限制下载。

**问题 5:**在 WinGate 代理服务器中,管理员不可以限制客户机访问时间。设置方法是:进入 WinGate 管理主界面,单击 Services 选项卡,双击 WWW Proxy server,弹出 WWW Proxy server properties 对话框;单击 Policies 选项卡,将 Default right 的选项改为“are ignored”,表示非窗口列中允许的用户权限均不能访问;单击 Add 按钮,弹出 Properties for new recipient 对话框,然后单击 Time 选项卡,单击 Specify times when this recipient has right 选项按钮,可以看到 Time 选项卡下有 Included times 和 Excluded time 列表框,Included time



列表框是设置允许使用时间段,系统到时会自动开启服务,而“Excluded time”列表框则是设置拒绝使用时间段,到时会自动关闭服务。设置拒绝时间段,单击 Excluded time 列表框的 Add 按钮,弹出 Time Slice 窗口,在该窗口设置所需的拒绝时间,单击 OK 按钮。使用同样方法,可设置允许上网时间段。

答案:

【问题 1】较大的硬盘、大容量的内存、两块网卡。

【问题 2】连接 Internet 的网卡的设置为:IP 地址为 222.152.199.33、子网掩码为 255.255.255.252、默认网关为 222.152.199.34、DNS 为 202.102.192.68;接入内部局域网的设置为:IP 地址为 192.168.10.1,其他参数可以不设置。

【问题 3】IP 地址不变,将默认网关改为 192.168.1.1、DNS 改为 202.102.192.68,并安装 WinGate 客户端。

【问题 4】在代理服务器中设置下载限制。

【问题 5】在代理服务器中指定游览时间。

例 3 阅读以下说明,回答问题 1~5,将答案填入对应的答案栏内。

【说明】

某小型公司已经建成了一个局域网,内部计算机的 IP 地址为 192.168.10.2~192.168.10.254,子网掩码为 255.255.255.0,DNS 和默认网关都没有设置。该公司在 ISP 申请了 Internet 接入,接入方式是以太网,ISP 分配给了一个固定的 IP 地址为 222.152.199.33、子网掩码为 255.255.255.252、默认网关为 222.152.199.34、DNS 为 202.102.192.68。该公司使用一台 PC 服务器作为代理服务器实现整个公司上网,代理服务器的操作系统是 Linux,代理软件是 Squid。下面是 Squid 的主要配置文件/etc/squid/squid.conf 内容片断:

```
http_port 3128
cache_mem 194 MB
cache_dir /cache1 4000 24 33
cache_access_log /usr/local/squid/logs/access.log
cache_log /usr/local/squid/logs/cache.log
dns_nameservers _____(1)_____
acl denyaddress src 192.168.10.99-192.168.10.105/255.255.255.255
acl all src 0.0.0.0/0.0.0.0
http_access deny denyaddress
http_access allow all
cache_mgr netsnake@963.net
```

【问题 1】代理服务器网络配置如何设置?

【问题 2】若采用传统代理方式,则客户机网络设置是否需要修改?是否需要安装客户端软件?若不需要安装客户端软件,则相关软件如何设置?(以 IE 为例)

【问题 3】代理服务器缓冲区放在哪里?大小是多少?

【问题 4】(1)处该填写什么内容?

【问题 5】在内部局域网中,哪些计算机不能通过代理访问 Internet?

分析: 该题主要考查基于 Linux 代理服务器的规划和管理。

问题 1: 同例 1 中的【问题 2】。

问题 2: 在传统代理中, 客户端网络设置比较简单, 只需要设置 IP 地址就可以了, 不需要安装客户端软件。但相关的应用软件(如 IE、CuteFTP 等)上必须要做相应设置, 主要有两个参数, 一个是代理服务器的 IP 地址和端口号。

问题 3: 代理服务器缓冲区放的位置和大小是由/etc/squid/squid.conf 文件中 cache\_dir 选项来指定的, 同时该参数还可指定目录结构, 定义方法是:

cache\_dir <目录> <大小> <一级目录数> <二级目录数>

“目录”指明了该交换空间的顶级目录, “大小”定义了可用的空间总量, 其单位是 Mb。因此, 在本例中, 代理服务器缓冲区放在/cache1, 大小为 4000M。

问题 4: dns\_nameservers 选项用来定义 Squid 进行域名解析时使用的域名服务器的, 因为在使用代理协议时, 客户端并不进行域名查询, 而是通过代理进行的。因此(1)处该填写 ISP 提供的域名服务器的地址, 即 202.102.192.68。

问题 5: 在 Squid 代理服务器通常通过两个选项配合起来实现访问控制的, 用选项 acl 来定义访问控制列表, 用 http\_access 来实施访问控制。在本例中, 有两条 acl 选项, 一条是定义源 IP 地址从 192.168.10.99 到 192.168.10.105, 另一条是定义源 IP 地址为任意地址。但接下为 http\_access 选项禁用了第一个地址空间, 但允许第二条, 因此在内部网络中主机地址为 192.168.10.99 到 192.168.10.105 不能访问 Internet。

答案:

【问题 1】连接 Internet 的网卡的设置为: IP 地址为 222.152.199.33、子网掩码为 255.255.255.252、默认网关为 222.152.199.34、DNS 为 202.102.192.68; 接入内部局域网的设置为: IP 地址为 192.168.10.1, 其他参数可以不设置。

【问题 2】客户机网络设置不需要修改, 也不需要安装客户端软件, 但相关软件需要作相应的设置。以 IE 为例, 需要设置代理服务器 IP 地址和端口号, IP 地址为 192.168.10.1, 端口号为 3128。

【问题 3】代理服务器缓冲区放在/cache1, 大小为 4000M。

【问题 4】202.102.192.68。

【问题 5】192.168.10.99~192.168.10.105。

### 3.6.3 同步练习

1. Squid 代理服务器的默认端口是什么?

A. 8080                      B. 3128                      C. 80                      D. 8888

2. \_\_\_\_\_ 是用于在 Linux 下实现代理服务器的软件。

A. ISA                      B. WinGate                      C. Sygate                      D. Squid

3. 阅读以下说明, 回答问题 1~5, 将答案填入对应的答案栏内。

【说明】

某小型公司已经建成了一个局域网, 内部计算机的 IP 地址为 192.168.1.2~192.168.1.254, 子网掩码为 255.255.255.0, DNS 和默认网关都没有设置。该公

公司在 ISP 处申请了 Internet 接入, 接入方式是以以太网, ISP 分配给了一个固定的 IP 地址为 222.152.199.33、子网掩码为 255.255.255.252、默认网关为 222.152.199.34、DNS 为 202.102.192.68。该公司使用一台 PC 服务器作为代理服务器以实现整个公司上网, 代理软件准备采用 WinGate 5.0, 代理方式采用透明代理, 网络拓扑结构图如图 3.94 所示。

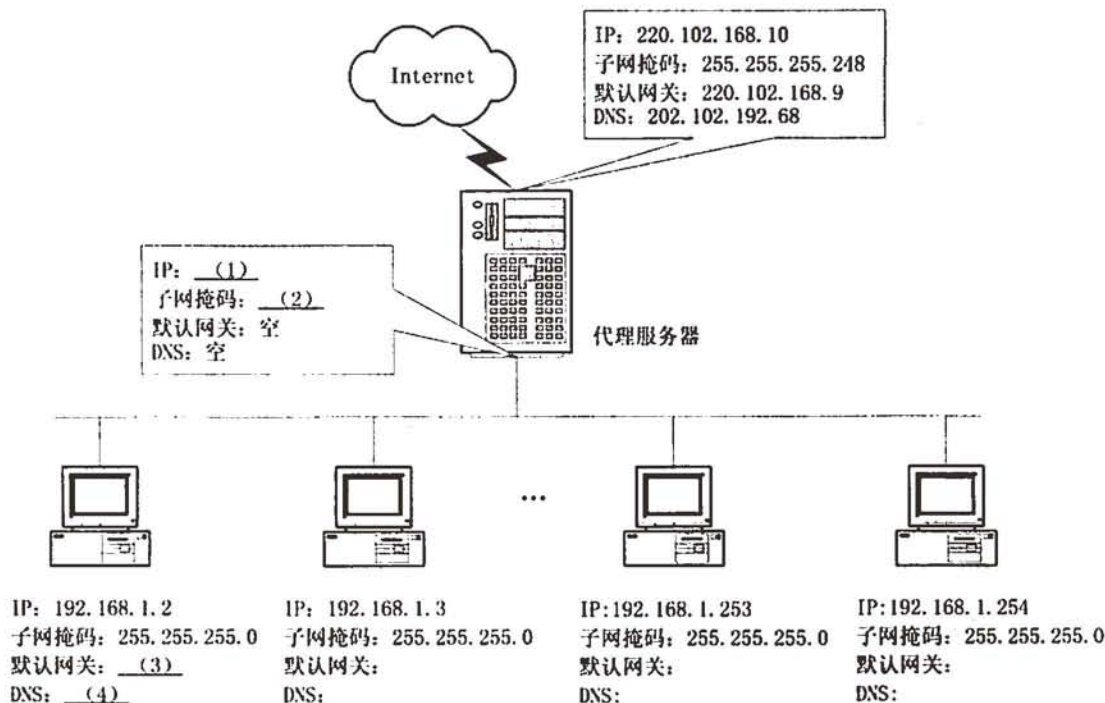


图 3.94 同步练习 1 拓扑图

【问题 1】(1)处该填写什么内容?

【问题 2】(2)处该填写什么内容?

【问题 3】(3)处该填写什么内容?

【问题 4】(4)处该填写什么内容?

【问题 5】需要安装何种软件并作何种设置? 若客户机使用 IE 浏览网页, 如何设置 IE。

4. 阅读以下说明, 回答问题 1~6, 将答案填入对应的答案栏内。

【说明】

在 Linux 下安装配置代理服务 Squid, Squid 服务程序/usr/sbin/squid 需要读取配置文件 /etc/squid/squid.conf, 以下是一个该文件的内容片断。

```
http_port 4444
cache_mem 32 MB
cache_dir /home/squid/cache 1024 16 256
cache_access_log /usr/local/squid/logs/access.log
cache_log /usr/local/squid/logs/cache.log
dns_nameservers 210.45.12.31
acl denyip dst 61.136.135.04/255.255.255.255
```

```
acl all scr 0.0.0.0/0.0.0.0
http_access deny denyip
http_access allow all
cache_mgr root@weboa.com.cn
```

【问题 1】客户机的 IE 的代理服务器端口号应设置为多少？

【问题 2】该代理服务器缓冲区放在哪里？大小是多少？能建多少一级目录，多少二级目录？

【问题 3】该代理服务器使用的域名服务器 IP 地址是什么？

【问题 4】文件中阴影的两行的作用是什么？

【问题 5】#squid -z 命令的作用是什么？

【问题 6】修改完配置文件后，如何使其立即生效？(不重新启动计算机)

### 3.6.4 同步练习参考答案

1. B

2. D

3.

【问题 1】192.168.1.1

【问题 2】255.255.255.0

【问题 3】192.168.1.1

【问题 4】202.102.192.68

【问题 5】需要安装 WinGate 客户端，IE 不需做任何设置

4.

【问题 1】4444

【问题 2】/home/squid/cache 1024 16 256

【问题 3】210.45.12.31

【问题 4】禁止所有的客户机的访问 IP 地址为 61.136.135.04 的站点

【问题 5】为 Squid 初始化 Cache 目录

【问题 6】#/etc/rc.d/init.d/squid restart

## 3.7 DHCP 服务器配置

### 3.7.1 考点辅导

#### 3.7.1.1 DHCP 基础

##### 1. DHCP 是什么？

动态主机分配协议(DHCP)是一个简化主机 IP 地址分配管理的 TCP/IP 标准协议。用户可以利用 DHCP 服务器管理动态的 IP 地址分配及其他相关的环境配置工作(如：DNS、



WINS、Gateway 的设置)。

在使用 TCP/IP 协议的网络上, 每一台计算机都拥有惟一的计算机名和 IP 地址。IP 地址(及其子网掩码)使用与鉴别它所连接的主机和子网, 当用户将计算机从一个子网移动到另一个子网的时候, 一定要改变该计算机的 IP 地址。如采用静态 IP 地址的分配方法将增加网络管理员的负担, 而 DHCP 可以让用户将 DHCP 服务器中的 IP 地址数据库中的 IP 地址动态地分配给局域网中的客户机, 从而减轻了网络管理员的负担。

在使用 DHCP 时, 整个网络至少有一台服务器上安装了 DHCP 服务, 其他要使用 DHCP 功能的工作站也必须设置成利用 DHCP 获得 IP 地址。图 3.95 所示是一个支持 DHCP 的网络实例。DHCP 是基于客户机/服务器模型设计的, DHCP 客户机和 DHCP 服务器之间通过收发 DHCP 消息进行通信。

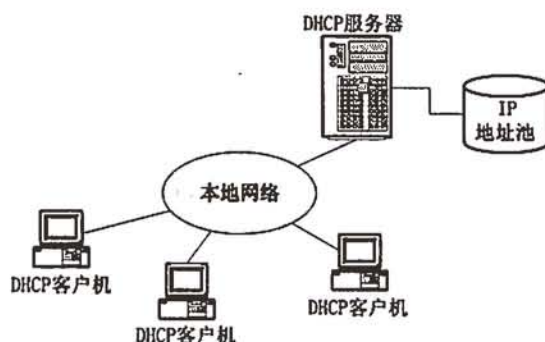


图 3.95 DHCP 服务工作原理

## 2. 使用 DHCP 的优点

### (1) 安全而可靠

DHCP 避免了因手工设置 IP 地址等参数可能产生的错误, 同时也避免了把一个 IP 地址分配给多台工作站所造成的地址冲突。

### (2) 网络配置自动化

使用 DHCP 服务器大大缩短了配置或重新配置网络中工作站所花费的时间。

### (3) IP 地址变更自动化

DHCP 地址租约的更新过程将有助于确定哪个客户的设置需要经常更新(如: 使用笔记本的客户经常更换地点), 且这些变更由客户机与 DHCP 服务器自动完成, 无须网络管理员干涉。

## 3. DHCP 相关的专业术语

(1) DHCP 客户: DHCP 客户是指通过 DHCP 来获得网络配置参数的 Internet 主机, 通常就是普通用户的工作站。

(2) DHCP 服务器: DHCP 服务器是提供网络设置参数给 DHCP 客户的 Internet 主机。

(3) DHCP/BOOTP 中继代理: 在 DHCP 客户和服务器之间转发 DHCP 消息的主机或路由器。

(4) 作用域: 作用域是一个网络中的所有可分配的 IP 地址的连续范围。它主要用来定义网络中单一的物理子网的 IP 地址范围。作用域是服务器用来管理分配给网络客户的 IP

地址的主要手段。

(5) 超级作用域：超级作用域是一组作用域的集合，它用来实现同一个物理子网中包含多个逻辑 IP 子网。在超级作用域中只包含一个成员作用域或子作用域的列表。然而超级作用域并不用于设置具体的范围。子作用域的各种属性需要单独设置。

(6) 排除范围：排除范围是不分配的 IP 地址序列。它保证在这个序列中的 IP 地址不会被 DHCP 服务器分配给客户。

(7) 租约时间：租约时间是 DHCP 服务器指定的时间长度，在这个时间范围内客户机可以使用所获得的 IP 地址。当客户机获得 IP 地址时租约被激活。在租约到期前客户机需要更新 IP 地址的租约，当租约过期或从服务器上删除时，租约停止。

(8) 选项类型：选项类型是 DHCP 服务器给 DHCP 工作站分配服务租约时分配的其他客户配置参数。经常使用的选项包括默认网关的 IP 地址、WINS 服务器及 DNS 服务器。一般在设置每个范围时这些选项都被激活。

#### 4. DHCP 服务器的工作原理

DHCP 客户使用两种不同的过程来与 DHCP 服务器通信并获得配置信息。DHCP 服务器是通过客户机租用网络地址来工作的，其租用过程的步骤随客户机是初始化还是续订其租约而不同。当客户计算机启动并尝试加入网络时，它将执行初始化过程。在客户机拥有租约之后将执行续订过程，但是需要使用服务器续订该租约。

##### (1) 初始化租约过程

启用 DHCP 的客户机首次启动时，会自动执行初始化过程以便从 DHCP 服务器获得租约，主要的几个过程分别介绍如下(如图 3.96 所示)。

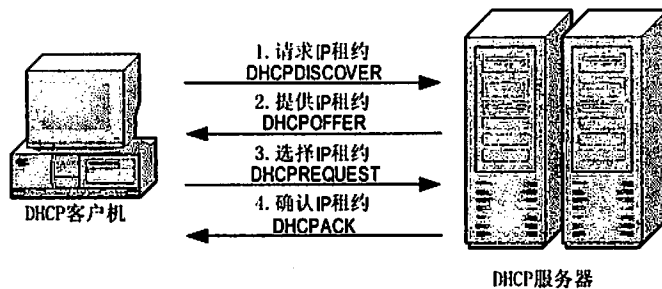


图 3.96 DHCP 初始化租约过程

① 请求 IP 租约：DHCP 客户机在本地子网中先发送 DHCP discover(DHCP 发现)消息，此消息以广播的形式发送，因为客户机还不知道 DHCP 服务器的 IP 地址。

② 提供 IP 租约：DHCP 服务器可通过包含有为客户端租约提供的 IP 地址的 DHCP 提供(DHCPOFFER)；在 DHCP 服务器收到 DHCP 客户机广播的 DHCP discover 信息后，它向 DHCP 客户机发送 DHCP offer(DHCP 提供)消息进行响应，在消息中包括一个可租用的 IP 地址。

③ 选择 IP 租约：一旦客户机收到 DHCP offer 信息，它发送 DHCP request(DHCP 请求)信息到服务器，表示它将使用服务器所提供的 IP 地址。

④ 确认 IP 租约：DHCP 服务器在收到 DHCP request 信息后，即发送 DHCP

positive(DHCP 确认)确认信息,以确定此租约成立,而且此信息中还包含其他 DHCP 选项信息。

客户机一旦接收到确认消息,就使用消息回复中的信息来配置其 TCP/IP 属性并加入网络。

在极少数情况下, DHCP 服务器可交替地向客户机返回 DHCP 否定确认消息。当客户机请求对于网络无效或重复的地址时可能会发生这种情况。如果客户机接收到否定确认消息,则当前的初始化过程失败。在这种情况下,客户机在第一步启动并重复如上所述的过程。

## (2) 租约续订过程

当 DHCP 客户机关闭并在相同的子网上重新启动时,它一般能获得和它关机之前的 IP 地址相同的租约。经过 50% 的客户机租约时间后,客户机会尝试通过 DHCP 服务器来续订其租约,具体步骤如下:

① 客户机直接向它所租用的服务器发送 DHCP 请求消息(DHCPRequest)以续订和扩展当前的地址租约。

② 如果可访问到服务器,它通常向客户机发送 DHCP 确认消息(DHCPACK),该客户机续订当前租约。同时,和初始租约过程中一样,其他 DHCP 选项信息也包含在该回复消息中。自客户机首先获得租约之后只要有选项信息发生变化,客户机就会相应地更新其配置。

③ 如果客户机不能与其最初的 DHCP 服务器通信,则客户机会一直等到它进入重新绑定状态。客户机在到达该状态时,会尝试通过任何可用的 DHCP 服务器来续订其当前租约。

④ 如果服务器用 DHCP 提供消息(DHCPoffer)进行响应以更新当前客户机租约,则客户机可根据提供服务器来续订其租约并继续运行。

⑤ 如果租约过期并且未联系到服务器,则客户机必须立即中止使用其租用的 IP 地址。

⑥ 客户机按照其初始启动操作期间使用的相同过程来获得新的 IP 地址租约。

## 5. DHCP 客户机的设置

DHCP 服务器安装设置完成后,客户机就可开始启用 DHCP 功能。

### (1) 启用 Windows 95/98 客户机的 DHCP 功能

① 右击【网上邻居】图标,在弹出的快捷菜单中选择【属性】命令,在弹出的对话框中,单击 TCP/IP 选项,单击【属性】按钮。

② 单击选中【自动获取 IP 地址】选项即可。

### (2) 启用 Windows 2000/XP/2003 客户机的 DHCP 功能

① 右击【网上邻居】图标,选择【属性】命令,在弹出的对话框中,右击【本地连接】图标,在出现的对话框中,单击【Internet 协议(TCP/IP)]选项,单击【属性】按钮。

② 单击选中【自动获取 IP 地址】选项即可。

### (3) 查看、更新和释放 IP 地址租约

在启用 DHCP 功能的 Windows 2000/XP 客户机要查看、更新和释放 IP 地址租约可以

使用 `ipconfig` 这一工具来完成。该诊断命令显示所有当前的 TCP/IP 网络配置值。该命令在运行 DHCP 系统上的特殊用途, 允许用户决定 DHCP 配置的 TCP/IP 配置值。

其命令格式是:

```
ipconfig [/all | /renew [adapter] | /release [adapter]]
```

参数:

`/all`: 产生完整显示。在没有该开关的情况下 `ipconfig` 只显示 IP 地址、子网掩码和每个网卡的默认网关值。

`/renew [adapter]`: 更新 DHCP 配置参数。该选项只在运行 DHCP 客户端服务的系统上可用。要指定适配器名称, 请键入使用不带参数的 `ipconfig` 命令显示的适配器名称。

`/release [adapter]`: 发布当前的 DHCP 配置。该选项禁用本地系统上的 TCP/IP, 并只 DHCP 客户端上可用。要指定适配器名称, 请键入使用不带参数的 `ipconfig` 命令显示的适配器名称。

如果没有参数, 那么 `ipconfig` 实用程序将向用户提供所有当前的 TCP/IP 配置值, 包括 IP 地址和子网掩码。该使用程序在运行 DHCP 的系统上特别有用, 允许用户决定由 DHCP 配置的值。

对于启用 DHCP 的 Windows 95 和 Windows 98 客户机, 请使用 `winipcfg` 命令的 `all`、`release` 和 `renew` 选项, 而不是 `ipconfig /all/release` 和 `ipconfig /renew` 命令来查看、释放或更新客户的 IP 配置租约。

### 3.7.1.2 Windows Server 2003 下 DHCP 服务器配置与管理

#### 1. DHCP 服务器的安装

安装 DHCP 服务器的步骤如下:

(1) 选择【开始】|【设置】|【控制面板】菜单项, 在【控制面板】对话框中双击【添加或删除程序】, 然后在出现的对话框中单击“添加/删除 Windows 组件”选项, 如图 3.97 所示。

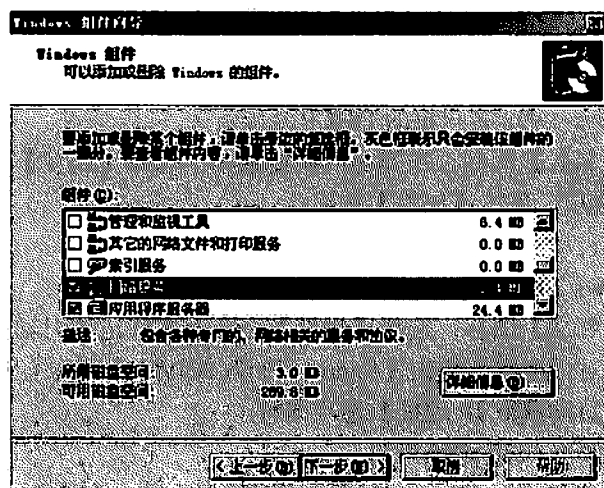


图 3.97 【Windows 组件】对话框



(2) 在【Windows 组件】对话框中,选中【网络服务】选项,然后单击【详细信息】按钮,在出现的【网络服务】对话框中,选中【动态主机配置协议(DHCP)】选项。单击【确定】按钮,如图 3.98 所示。

(3) 单击【下一步】按钮,将 Windows Server 2003 安装光盘置入光驱,即开始安装和配置 DHCP 组件。

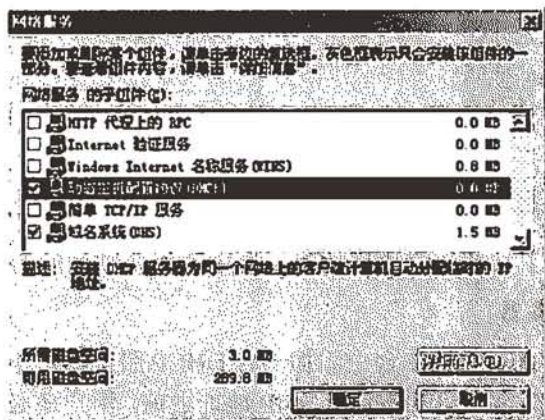


图 3.98 【网络服务】对话框

(4) 安装完成,单击【完成】按钮就当回到【添加/删除程序】对话框后,单击【关闭】按钮就完成 DHCP 服务的安装。

安装结束后,会在【开始】|【程序】|【管理工具】菜单中增加 DHCP 菜单项。

## 2. 添加 DHCP 服务器

在安装 DHCP 服务后,用户必须首先添加一个授权的 DHCP 服务器,并在服务器中添加作用域,设置相应的 IP 地址范围及选项类型,以便 DHCP 客户机在登录到网络时,能够获得 IP 地址租约和相关选项的设置参数。

(1) 选择【开始】|【程序】|【管理工具】| DHCP 菜单项,打开 DHCP 控制台窗口,如图 3.99 所示。

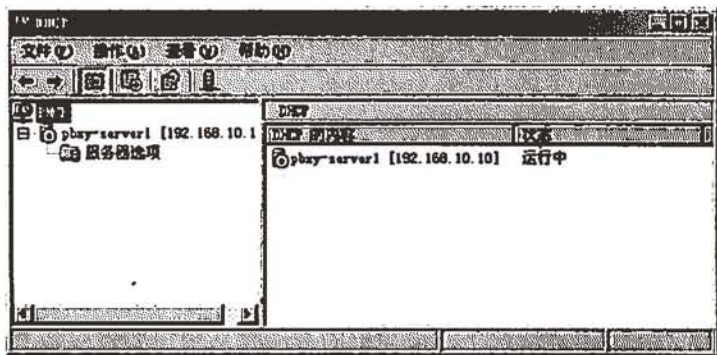


图 3.99 DHCP 控制台窗口

(2) 选择【操作】|【添加服务器】菜单命令,打开【添加服务器】对话框,如图 3.100 所示。

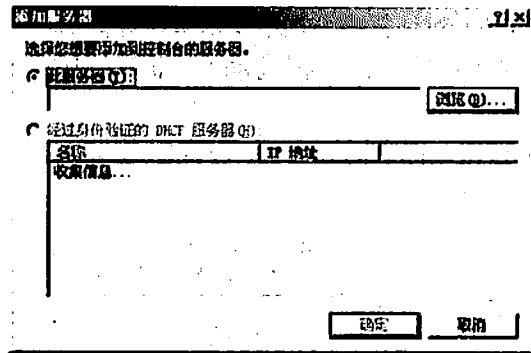


图 3.100 【添加服务器】对话框

(3) 在【添加服务器】对话框中,在【此服务器】文本框中填写 DHCP 服务器名或 IP 地址,也可单击【浏览】按钮,在出现的对话框中选择要添加的 DHCP 服务器。

### 3. 授权 DHCP 服务器

用户只是简单地在 DHCP 控制台添加一台 DHCP 服务器还不能使该服务器正常工作。在 DHCP 服务器为客户机动态地分配 IP 地址之前,用户还必须为新添加的服务器进行授权。这里的授权是指,为了保证网络的安全 Windows Server 2003 服务器系统只允许那些已经被授权的 DHCP 服务器在网络中发行 IP 地址。而没有被授权的 DHCP 服务器不能为客户机提供服务。如果用户是在 Active Directory 的主域控制器上安装 DHCP 服务,在用户第一次向 DHCP 控制台添加该服务时,服务器便会自动为新添加的 DHCP 服务器进行授权。不过,用户可以为该主域控制器同时授权多个 DHCP 服务器来为网络客户机提供服务。

#### (1) 授权的概念

DHCP 服务器在网络上正确配置和授权使用时,将提供有用且计划好的管理服务。但是,当错误配置或未授权的 DHCP 服务器被引入网络时,它可能会带来问题。例如,如果启动了未授权的 DHCP 服务器,它可能开始为客户机租用不正确的 IP 地址或者否认尝试更新当前地址租约的 DHCP 客户机。这些配置中的任何一个都可能导致启用 DHCP 的客户机产生更多的问题。例如,从未授权的服务器获取配置租约的客户机将找不到有效的域控制器,致使客户机难以成功登录到网络上。

为避免在 Windows Server 2003 中出现这些问题,在它们为客户机提供服务之前需要管理员在网络中验证服务器是否合法。这样就避免了由于在错误网络上运行带有不正确或正确配置的 DHCP 服务器而导致的大多数意外破坏。

如果用户配置了 Active Directory,那么作为 DHCP 服务器运行的所有计算机在目录服务中获得授权及为客户机提供 DHCP 服务之前,必须是域控制器或者域成员服务器。

要将计算机控权为 DHCP 服务器,可使用下列处理步骤:

① 使用具有企业管理特权的账户或者使用已获得委派可向企业的 DHCP 服务器授权的账户登录到网络。在大多数情况下,最简单的方法是从用户要授权新 DHCP 服务器的计算机登录到网络。这可以确保已授权计算机的其他 TCP/IP 配置已在授权之前正确建立。通常,用户可以使用作为企业管理员组成员的账户。当 NetServices 容器对象存储在 Active Directory 服务的企业根位置时,用户使用的账户必须允许其有访问该对象的“完全控制”

权限。

② 启动 DHCP 控制台并选择作为 DHCP 服务器运行的计算机,该 DHCP 服务器是用户想在目录服务数据库中作为授权服务器添加的。如果本地计算机未获得授权,那么在启动 DHCP 控制台时,请选择【本地计算机】选项用于连接。如果网络上的另一台计算机获得授权,请选择【远程计算机】选项。

授权 DHCP 服务器时,服务器计算机被添加到在目录服务数据库中维护的授权 DHCP 服务器列表中。用户可通过使用 Active Directory 站点和服务控制台检查属性来验证服务器是否已被添加。这些属性位于【配置】项下,它是在企业根的下列文件夹位置中保存的全局容器。

## (2) 为创建的 DHCP 服务器授权

在理解了授权的作用之后,用户即可为添加的 DHCP 服务器进行授权的操作了,以便使该服务器具有分配动态 IP 地址的权限。

下面是对 DHCP 服务器授权的具体操作步骤。

① 打开 DHCP 控制台窗口,在控制台目录树中右击 DHCP 根节点,从弹出的快捷菜单中选择【管理授权的服务器】命令,打开【管理授权的服务器】对话框,如图 3.101 所示。

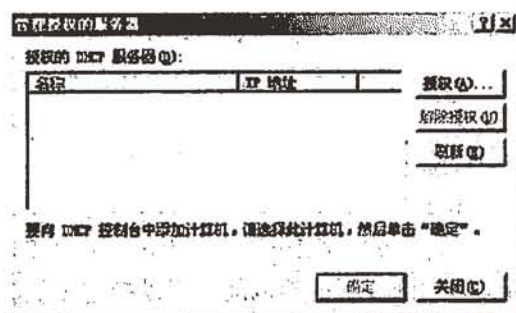


图 3.101 【管理授权的服务器】对话框

② 在【管理授权的服务器】对话框中,用户可以解除对已经被授权的 DHCP 服务器的授权,同时也可以为新的 DHCP 服务器进行授权。单击【授权】按钮后,系统将打开【授权 DHCP 服务器】对话框,如图 3.102 所示。

③ 在【授权 DHCP 服务器】对话框中,用户需要在【名称或 IP 地址】文本框中输入刚刚添加的 DHCP 服务器的名称或 IP 地址,也可以输入本机的计算机名称。单击【确定】按钮后,系统将打开【确认授权】对话框,如图 3.103 所示。

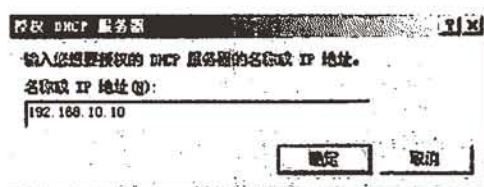


图 3.102 【授权 DHCP 服务器】对话框

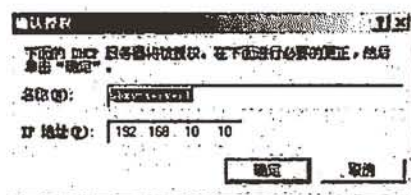


图 3.103 【确认授权】对话框

④ 在该对话框中,系统将显示出用户指定的主机的名称及该主机的 IP 地址信息,以使用户确认将要授权的 DHCP 服务器的正确性。单击【确定】按钮系统将返回到【管理授

权的服务器】对话框。授权的 DHCP 服务器已经被加入到了【授权的 DHCP 服务器】列表框中，单击【关闭】按钮关闭对话框。

#### 4. 创建作用域

在创建了 DHCP 服务器并为它授权后，用户还需要进行另一项重要的工作，即创建作用域。作用域是指指派给请求动态 IP 地址的计算机的 IP 地址的范围。用户只有在创建了一个新的作用域后，DHCP 服务器才能拥有可被分配的 IP 地址，而这些地址都储存在地址池中。当客户机发出地址请求后，DHCP 服务器将和客户机签定一个地址租约，这样客户机将会以租借的形式来使用临时的 IP 地址。

##### (1) 作用域概述

作用域是对使用 DHCP 服务的子网进行的计算机管理性分组。管理员首先为每个物理子网创建作用域，然后使用该作用域定义由客户机使用的参数。作用域具有下列属性。

- IP 地址的范围：可在其中加入或排除用于 DHCP 服务租约的地址。
- 惟一的子网掩码：用于确定给定 IP 地址的子网。
- 租约期限：指派给动态接收分配的 IP 地址的 DHCP 客户机。

##### (2) 创建作用域

DHCP 作用域由给定子网上 DHCP 服务器可以租用给客户机的 IP 地址池组成。例如，213.248.173.113~213.248.173.129。每个子网只能有一个具有连续 IP 地址范围的单个 DHCP 作用域。要在单个作用域或子网内使用多个地址范围以提供 DHCP 服务，必须首先定义作用域，然后设置所需的任何排除范围。

管理员应该在不希望 DHCP 服务器提供或用于 DHCP 指派的作用域中设置任何 IP 地址排除范围。例如，可通过创建 168.168.168.1~168.168.168.22 的排除范围，将其中的 10 个地址排除在外。通过为这些地址设置排除范围，可以指定在从服务器上请求租用配置时永远不为 DHCP 客户机提供这些地址。排除的 IP 地址可能是网络上的有效地址，但这些地址只能是通过在不使用 DHCP 获取地址的主机上手动配置的。

定义作用域以后，用户可通过另外配置作用域，以排除不必租给 DHCP 客户机的任何其他 IP 地址。应该为所有必须静态配置的设备使用排除范围。排除范围应包含管理员手动指派给其他 DHCP 服务器、非 DHCP 客户机、无盘工作站或者路由和远程访问及 PPP 客户机的所有 IP 地址。也可以选择为网络上的指定计算机或设备的永久租约指派保留某些 IP 地址。

创建作用域的主要作用即是为服务器指定和配置好可分配的 IP 地址。因此在创建新的 DHCP 服务器的操作中创建作用域的工作至关重要，它关系到 DHCP 是否拥有可分配的 IP 地址。

下面是创建 DHCP 作用域的操作步骤：

① 打开 DHCP 控制台窗口，在控制台树中右击要创建作用域的 DHCP 服务器，从弹出的快捷菜单中选择【新建作用域】命令，打开【欢迎使用新建作用域向导】对话框，如图 3.104 所示。

② 单击【下一步】按钮，系统将打开【作用域名】对话框。在该对话框中，用户需要在【名称】文本框中输入作用域的名称，并在【描述】文本框中输入一些说明性文字，



如图 3.105 所示。

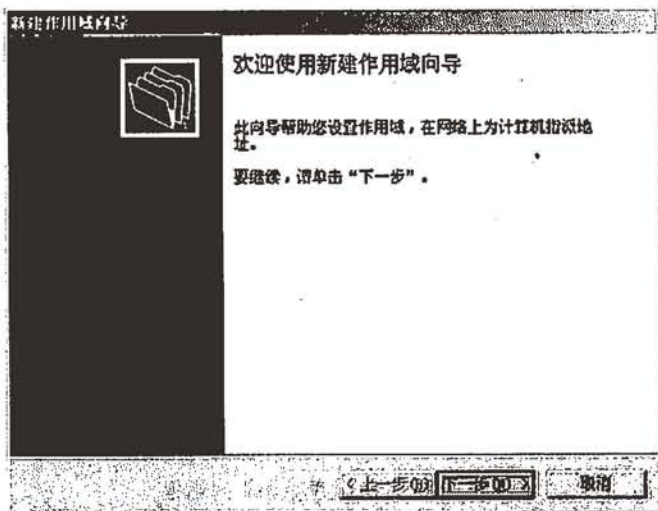


图 3.104 【欢迎使用新建作用域向导】对话框

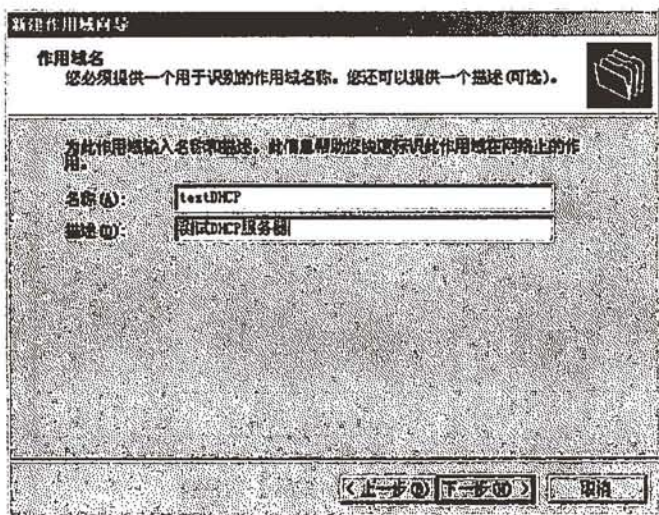


图 3.105 【作用域名】对话框

③ 单击【下一步】按钮后，系统将打开【IP 地址范围】对话框。在该对话框中，用户可以指定作用域的地址范围。在【输入此作用域分配的地址范围】选项区域的【起始 IP 地址】和【结束 IP 地址】文本框中分别输入作用域的起始地址和结束地址。通过输入合适的子网掩码，用户可以调整已定义时 IP 地址中有多少位用作网络的 ID 及多少位用作主机的 ID。不同的子网掩码决定了网络客户机属于不同的网络。同时用户还可以通过调整【长度】文本框的数值来完成子网掩码的设置，如图 3.106 所示。

④ 单击【下一步】按钮进入【添加排除】对话框，如图 3.107 所示。在该对话框中，用户可以定义服务器不分配的 IP 地址。排除范围应当包括所有手工分配给其他 DHCP 服务器、非 DHCP 客户机、无盘工作站或 RAS 和 PPP 客户机的 IP 地址。如果有要排除的 IP 地址，按下述方法定义。

**新建作用域向导**

**IP 地址范围**  
您通过确定一组连续的 IP 地址来定义作用域地址范围。

输入此作用域分配的地址范围。

起始 IP 地址(S): 192.168.10.20

结束 IP 地址(E): 192.168.10.240

子网掩码定义 IP 地址的多少位用作网络/子网 ID, 多少位用作主机 ID。您可以使用长度或 IP 地址来指定子网掩码。

长度(L): 24

子网掩码(M): 255.255.255.0

< 上一步(B) 下一步(N) > 取消

图 3.106 【IP 地址范围】对话框

**新建作用域向导**

**添加排除**  
排除是指服务器不分配的地址或地址范围。

键入您想要排除的 IP 地址范围。如果您想排除一个单独的地址, 则只在“起始 IP 地址”键入地址。

起始 IP 地址(S): 192.168.10.200 结束 IP 地址(E):

排除的地址范围(R): 192.168.10.100 到 192.168.10.120

添加(A) 删除(D)

< 上一步(B) 下一步(N) > 取消

图 3.107 【添加排除】对话框

在【起始 IP 地址】文本框中输入排除范围的 IP 起始地址, 在【结束 IP 地址】文本框中输入排除范围的 IP 结束地址, 然后单击【添加】按钮。如果有多个排除范围, 使用同样方法定义它们。

要排除单个 IP 地址, 只需要在【起始地址】文本框中输入该 IP 地址, 而【结束地址】文本框保持为空, 然后单击【添加】按钮即可。

要从排除范围中删除 IP 地址或 IP 地址范围, 在【排除的地址范围】列表框中单击该地址, 然后单击【删除】按钮即可。

⑤ 单击【下一步】按钮, 进入【租约期限】对话框。租约期限指定了客户机使用 DHCP 服务器所分配的 IP 地址的时间。要指定作用域中 IP 地址的租用时间, 可通过微调框定义 IP 地址租用时间的“天”、“小时”和“分钟”数值, 如图 3.108 所示。

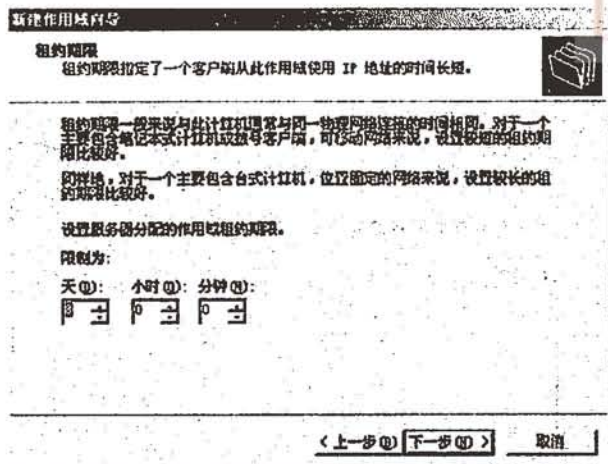


图 3.108 【租约期限】对话框

⑥ 单击【下一步】按钮，将打开【配置 DHCP 选项】对话框。要想让网络客户使用作用域，必需配置最常用的 DHCP 选项，这些选项包括网关、DNS 服务器和 WINS 设置等。要想立即配置这些 DHCP 选项，可选择【是，我想现在配置这些选项】单选按钮，如图 3.109 所示。

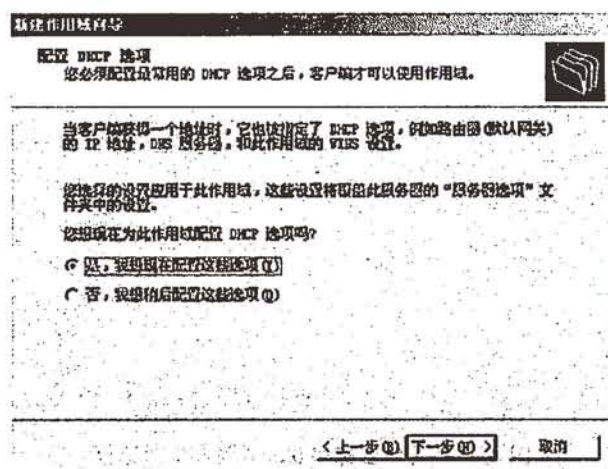


图 3.109 【配置 DHCP 选项】对话框

⑦ 单击【下一步】按钮，在打开的【路由器(默认网关)】对话框中可配置作用域的网关(或路由器)。在【IP 地址】文本框中输入网关地址，然后单击【添加】按钮添加网关。要删除已有的网关，可在网关列表框中单击该网关地址，然后单击【删除】按钮即可。如果管理员所在的网络不需要路由器，可以直接单击【下一步】跳过该步操作，如图 3.110 所示。

⑧ 单击【下一步】按钮，将打开【域名称和 DNS 服务器】对话框。在【父域】文本框中，用户需要输入父域的名称。如果本机为根域的控制域没有父域存在，可以直接输入本地域名。

在【服务器名】文本框中输入本地 DNS 服务器的名称后单击【解析】按钮，系统会将

已经配置的 DNS 服务器的 IP 地址显示在【IP 地址】文本框中, 用户只需单击【添加】按钮即可将该地址加入到 DNS 服务器列表中, 如图 3.111 所示。

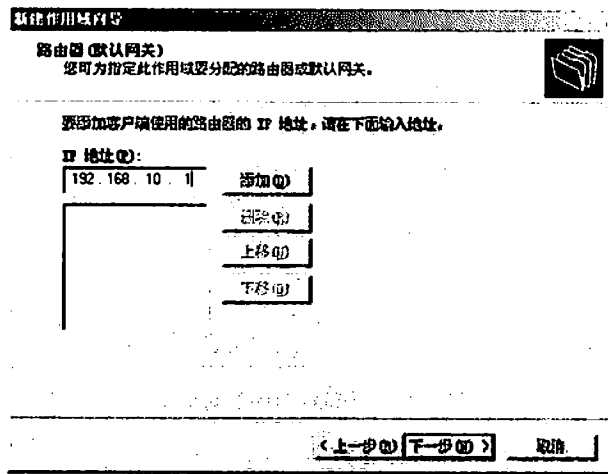


图 3.110 【路由器(默认网关)】对话框

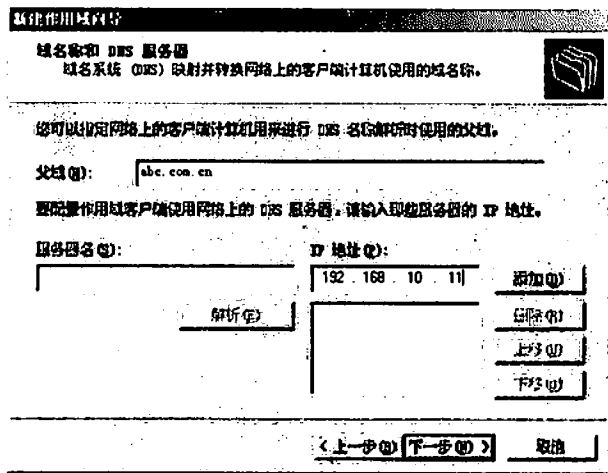


图 3.111 【域名称和 DNS 服务器】对话框

⑨ 单击【下一步】按钮后, 系统将打开【WINS 服务器】对话框。在该对话框中, 用户可以输入 WINS 服务器地址。WINS 服务器可以将 Windows 客户的计算机名称转换成相应的 IP 地址。单击【解析】按钮后, 系统将该 WINS 服务器对应的 IP 地址显示在【IP 地址】文本框中, 最后单击【添加】按钮将该地址加入到地址列表中, 如图 3.112 所示。

⑩ 完成 WINS 服务器设置后单击【下一步】按钮打开【激活作用域】对话框, 从中选中【是, 我想现在激活此作用域】单选按钮, 如图 3.113 所示。单击【下一步】按钮可立即激活此作用域, 这样【创建作用域向导】就完成了创建过程。系统将打开【正在完成新建作用域向导】对话框。用户只需单击【完成】按钮关闭【创建作用域向导】即可。

**注意:** 如果用户在创建作用域时没有很好地设置其内容, 可在作用域创建之后, 通过其属性对话框来修改设置。但是, 在修改地址范围时一般不应缩小其地址范围,



因为缩小地址范围可能导致 DHCP 客户租约地址的失败。

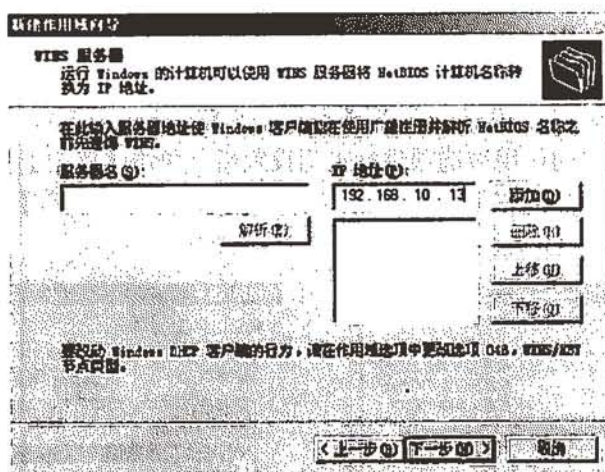


图 3.112 【WINS 服务器】对话框

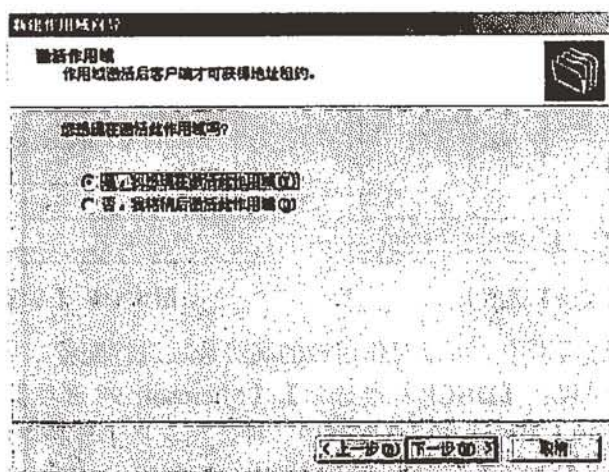


图 3.113 【激活作用域】对话框

## 5. 配置作用域

用户在创建了新的作用域后, 还需要对作用域选项进行一些相关的配置才能正常启动作用域中众多的选项功能。

### (1) 设置作用域选项

要配置作用域选项, 可参照下面的操作步骤。

① 选择【开始】|【程序】|【管理工具】| DHCP 菜单项, 打开 DHCP 控制台。在目录树中单击服务器节点并展开【作用域】节点及其子节点。右击选定的【作用域选项】节点, 从打开的快捷菜单中选择【配置选项】命令, 打开【作用域选项】对话框并从中选择【常规】选项卡, 如图 3.114 所示。

② 在【可用选项】列表框中, 当用户选中了某选项时, 系统将自动在【数据输入】

选项区域中打开该选项对应的设置。例如,选中【005 名称服务器】复选框后,在【数据输入】选项区域中系统会让用户输入名称服务器的新 IP 地址及服务器名称。用户在【IP 地址】文本框中输入新的 IP 地址,然后单击【添加】按钮将该地址添加到名称服务器列表中。用户也可以在【服务器名】文本框中输入某台服务器的名称,然后单击【解析】按钮,系统会自动将该服务器对应的 IP 地址解析到【IP 地址】文本框中。

③ 用户对所选定的作用域选项进行正确设置后,单击【确定】按钮以使设置生效。

④ 对常规选项设置完毕后,单击【高级】标签,打开【高级】选项卡,如图 3.115 所示。

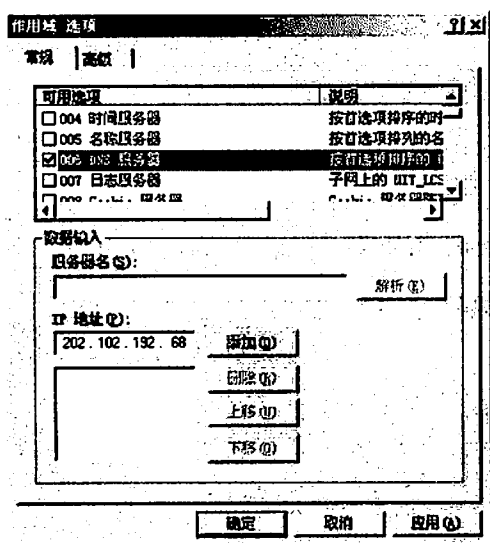


图 3.114 【常规】选项卡

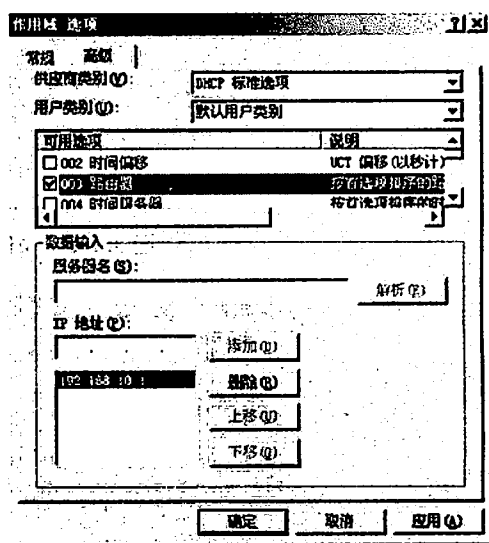


图 3.115 【高级】选项卡

⑤ 在【高级】选项卡中,可以对作用域的高级选项进行配置。其中在【供应商类别】下拉列表框中,用户可以在【DHCP 标准选项】、【Microsoft 98 选项】、【Microsoft 2000 选项】和【Microsoft 选项】4 种选项中选择其中一种。当选择了一种供应商类别后,其对应的可选项将显示在【可用选项】列表框中。如果用户已创建了 DHCP 服务器以及作用域的话,在【用户类别】下拉列表框中,系统会默认设置该选项为【默认用户类别】。

⑥ 如同在【常规】选项卡中的设置操作一样,在【可用选项】列表框中选定某选项后,可在【数据输入】选项区域中对该选项进行相应的设置。

⑦ 完成所有设置后,单击【确定】按钮以使设置生效。

## (2) 保留特定 IP 地址

有些时候,在 DHCP 网络中需要给某一台或几台 DHCP 客户端固定专用的 IP 地址,这就需要通过 DHCP 服务器提供的“保留”功能来实现。当这个 DHCP 客户端每次向 DHCP 服务器请求获得 IP 地址或更新 IP 地址租期时, DHCP 服务器都会给该 DHCP 客户端分配同一个的 IP 地址。保留特定 IP 地址的操作步骤如下:

① 选择【开始】|【程序】|【管理工具】| DHCP 菜单项,打开 DHCP 控制台。在目录树中单击服务器节点并展开“作用域”节点及其节点。右击选定的“保留”节点,从弹出的快捷菜单中选择【新建保留】命令,打开【新建保留】对话框,如图 3.116 所示。

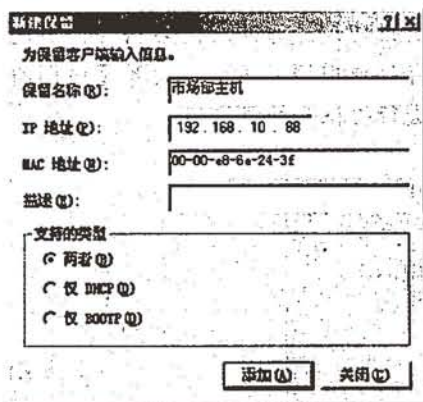


图 3.116 【新建保留】对话框

② 在【新建保留】对话框中输入保留名称、IP 地址、MAC 地址、说明并选择支持的类型。

在【保留名称】文本框中输入用于标识 DHCP 客户端的名称，该项既可以是 DHCP 客户端的真实名称，也可以是自定义的名称；在【IP 地址】文本框中输入要保留给该 DHCP 客户端的 IP 地址；在【MAC 地址】文本框中输入该 DHCP 客户端网卡的 MAC 地址，网卡的 MAC 地址是一个 12 位十六进制数，每块网卡地址是惟一的，它一般在出厂时标注在网卡上，在 Windows 95/98/Me 计算机上，可以利用 Winipcfg 测试工具测得，在 Windows NT/2000/XP/2003 系统的客户端，需要进入 DOS 提示符下，输入 ipconfig/all 命令来获得；【说明】用于在必要时输入一些辅助说明性文字；【支持的类型】用于设置该客户端是否必须支持 DHCP 服务。其中 BOOTP 主要用于无盘工作站，因此如果该客户端是以无盘方式工作，则选择【仅 BOOTP】一项，否则选择【仅 DHCP】一项，当无法确定时可以选择【两者】一项。

③ 输入完毕后，单击【添加】按钮可以保留一个 IP 地址给特定 DHCP 客户端来使用。

### (3) 协调作用域

协调作用域信息就是协调 DHCP 数据库中的作用域信息与注册表中的相关信息的一致性，如果不一致，系统将提示管理员修复错误将其协调一致，以免出现地址分配错误。

下面是协调作用域的操作步骤。

① 打开 DHCP 控制台窗口，在控制台树中展开要协调作用域的服务器。右击要协调的作用域，从弹出的快捷菜单中选择【协调】命令，打开【协调】对话框，如图 3.117 所示。

② 在【协调】对话框中，单击【验证】按钮即可将数据库中的作用域信息与注册表中的信息比较，如果一致则会出现一个 DHCP 对话框，单击【确定】按钮即可，如图 3.118 所示。

③ 如果作用域不一致，在列表框中就会列出所有不一致的 IP 地址，且【验证】按钮变为【协调】按钮。要修复不一致性，可先选择需要协调的 IP 地址，然后单击【协调】按钮即可。

④ 单击【确定】按钮关闭对话框。

注意：上面所讲是对单个作用域进行协调，如果某个服务器有多个作用域，管理员也

可以同时对它们进行协调。方法是：右击要协调的服务器，从弹出的快捷菜单中选择【协调所有的作用域】命令，打开【协调所有的作用域】对话框，然后按照上面的方法进行验证和协调即可。

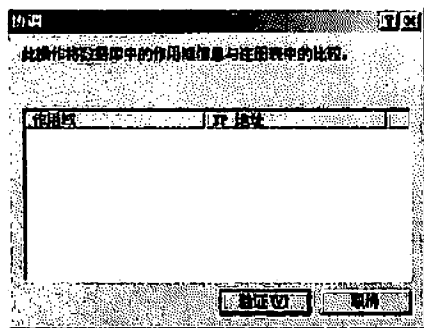


图 3.117 协调作用域



图 3.118 协调作用域结果

#### (4) 删除作用域

删除作用域就是从 DHCP 服务器中彻底地清除作用域中的 IP 地址对 DHCP 客户的分配。但是，删除作用域之前请务必停用作用域足够长的时间，以便能将客户机转移到不同的作用域。一旦所有客户机均已移动或强制在另一个作用域中搜索，管理员就可以安全地删除非活动的作用域。

要删除作用域，用户可以打开 DHCP 控制台窗口，在控制台目录树中展开所需服务器，右击要删除的作用域，从弹出的快捷菜单中选择【删除】命令即可。

### 6. 创建超级作用域

在 Windows Server 2003 中，用户除了可以使用 DHCP 服务器中标准的作用域来进行地址分配和地址管理外，还可以使用超级作用域来更好地分配和管理网络地址。因为，超级作用域允许用户将几个不同的作用域在逻辑上组合在一起并使用单一的作用域名称，这样通过超级作用域用户就可以对多个逻辑网进行管理。

#### (1) 超级作用域的概念

超级作用域是可以通过 DHCP 控制台创建和管理的 Windows Server 2003 的 DHCP 服务器的管理功能。使用超级作用域，可以将多个作用域组合为单个管理实体。使用此功能，DHCP 服务器可以在使用多个逻辑 IP 网络的单个物理网段(如单个以太网的局域网段)支持 DHCP 客户机。在每个物理域网或网络上使用多个逻辑 IP 网络时，这种配置通常被称为多网。它还能支持位于 DHCP 和 BOOTP 中继代理远端的远程 DHCP 客户机，并在中继代理远端的网络上使用多网配置。

在全网配置中，可以使用 DHCP 超级作用域来组合并激活网络上使用的单独作用域范围内的 IP 地址。这种情况下，DHCP 服务器计算机可以为单个物理网络上的客户机激活并提供来自多个作用域的租约。

超级作用域可以解决多网结构中的某种 DHCP 配置问题。例如，当前活动作用域的可用地址池几乎已耗尽，需要向网络中添加更多的计算机。最初的作用域包括指定地址类别的单个 IP 网络的一段完全可寻址范围，需要使用另一个网络地址范围以扩展同一物理网段



的地址空间。

## (2) 创建超级作用域

由于超级作用域可以包含其他分离的作用域的 IP 地址, 所以当管理员需要使用另外一个 IP 网络地址范围以扩展同一个物理网段的地址空间时, 就可以通过创建超级作用域来解决问题。

注意: 服务器要至少包含一个已创建的作用域, 新建超级作用域的命令才能使用。

要创建超级作用域, 可以参考以下步骤。

① 打开 DHCP 控制台窗口, 在控制台目录树中单击想要创建超级作用域的 DHCP 服务器。选择【操作】菜单中的【新建超级作用域】命令, 打开【新建超级作用域向导】对话框, 如图 3.119 所示。

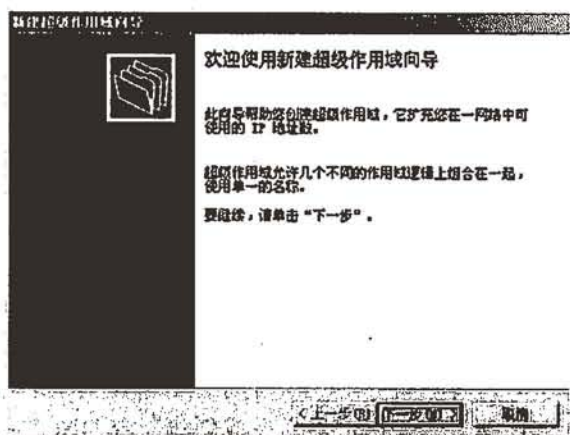


图 3.119 【新建超级作用域向导】对话框

② 在打开的【超级作用域名】对话框中输入超级作用域的名称, 如图 3.120 所示。

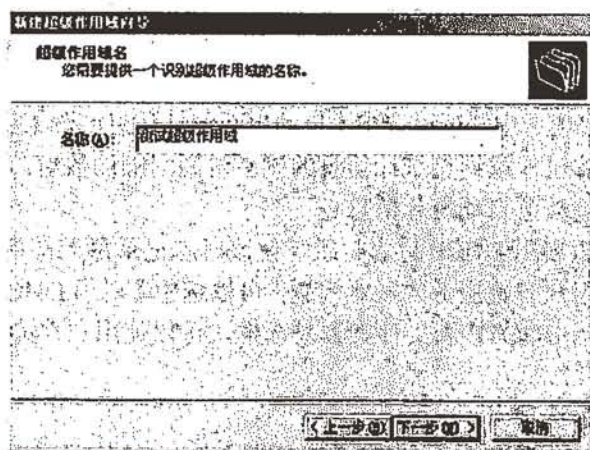


图 3.120 【超级作用域名】对话框

③ 单击【下一步】按钮, 打开【选择作用域】对话框, 如图 3.121 所示, 在该对话框中可选择该超级作用域所要包含的成员作用域(或称子作用域)。在【可用作用域】列表

中选择作用域时,如果需要选择多个作用域,可在按下 Shift 的同时单击作用域来选择多个连续作用域,或在按下 Ctrl 键的同时单击作用域来选择多个不连续作用域。

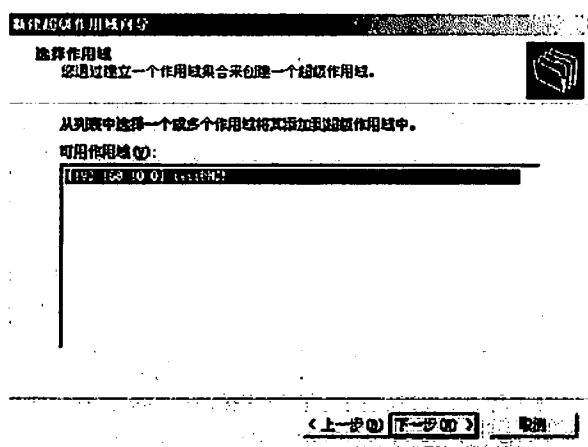


图 3.121 【选择作用域】对话框

④ 单击【下一步】按钮,系统将打开【创建完成】对话框,显示出所设置的作用域选项,单击【完成】按钮即可完成创建过程。

#### 7. 设置 DHCP 服务器的属性

配置一台 DHCP 服务器的属性在创建该服务器的整个过程中是最关键的一步工作。合适的属性配置能够保证该服务器正常、顺利地运行,也只有这样 DHCP 服务器才能对客户机的地址请求做出应答——为客户机分配一个可用的动态 IP 地址。对 DHCP 服务器的属性中一些关键的项目进行合理地设置是用户最后完成创建一台 DHCP 服务器的必要的工作。

下面将介绍如何对 DHCP 服务器的属性进行设置。

##### (1) 设置【常规】选项卡

① 打开【开始】菜单,选择【管理工具】|DHCP 命令,打开 DHCP 控制台窗口。右击选定的服务器,从弹出的快捷菜单中选择【属性】命令,打开该服务器的属性对话框,如图 3.122 所示。

② 在【常规】选项卡中,可以选中【自动更新统计信息间隔】复选框,然后通过【小时】和【分钟】微调按钮任意调整统计信息的刷新时间间隔的数值。这样 DHCP 服务器将按用户设定的时间间隔数值自动统计信息。

③ 如果用户希望启用 DHCP 日志记录,使该日志记录每天都将服务器的活动记录到一个文件中以供解答用户有关服务的疑难问题,可以选中【启用 DHCP 审核记录】复选框。另外,如果选中【显示 BOOTP 表文件夹】复选框,可以使用户在 DHCP 控制台窗口中查看到 BOOTP 文件夹消息。

##### (2) 设置【DNS】选项卡

① 在选定的 DHCP 服务器的【属性】对话框中打开【DNS】选项卡,如图 3.123 所示。

② 在【DNS】选项卡中,如果用户希望 DNS 服务器的正向和反向查找能够在客户从 DHCP 服务器那里获得租约时自动更新,可以选中【根据下面的设置启用 DNS 动态更新】复选框。该功能包括两种可选方式:根据客户请求更新方式和总是动态更新 DNS 和 PTR

记录的方式。用户可以根据需要选择【只有当 DHCP 客户端请求时才动态更新 DNS 和 PTR 记录】单选按钮或【总是动态更新 DNS 和 PTR 记录】单选按钮中的一个,以便使用该方式启用 DNS 客户信息更新功能。

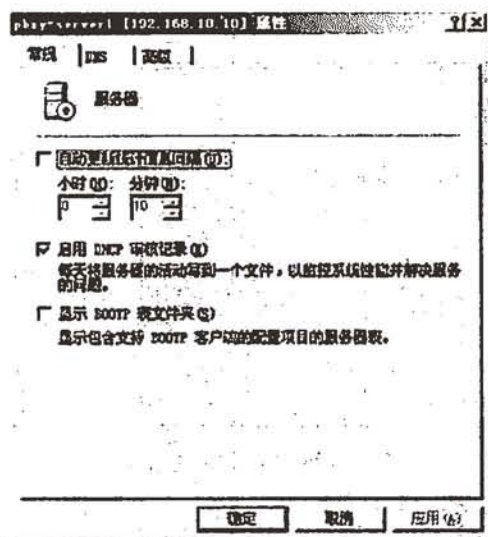


图 3.122 DHCP 服务器的属性对话框

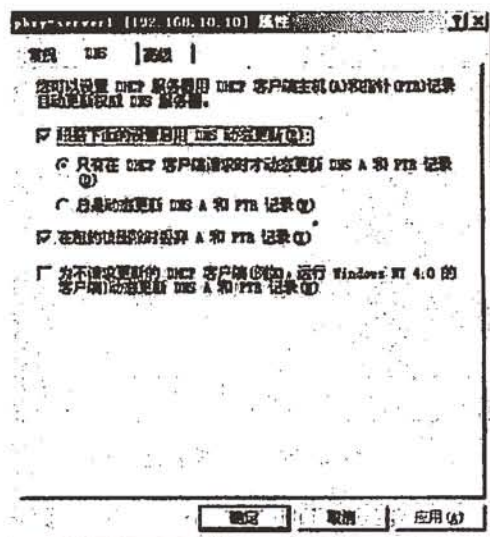


图 3.123 【DNS】选项卡

### (3) 设置【高级】选项卡

① 在选定的 DHCP 服务器的属性对话框中打开【高级】选项卡,如图 3.124 所示。

② 在【高级】选项卡中,如果希望 DHCP 把 IP 地址租给客户之前,DHCP 服务器能够对将要分配的 IP 地址进行一定次数的冲突检测可以通过【冲突检测次数】微调框来调整冲突检测的次数,以使 DHCP 按照指定的次数对 IP 地址进行检测。

③ 如果用户希望更改 DHCP 中的数据库和审核文件在硬盘中的存储位置,可以分别在【审核日志路径】文本框和【数据库路径】文本框中输入指定的完整路径。另外,还可以单击【浏览】按钮,从打开的对话框中为审核日志或数据库选择一个存储路径。

④ 如果需要更改 DHCP 服务器连接的绑定,可单击【绑定】按钮,系统将打开【绑定】对话框。在该对话框中,可以选择 DHCP 服务器为客户提供服务所支持的链接,单击【确定】按钮完成所有属性设置操作,如图 3.125 所示。

### 8. 停止、启动和重新启动 DHCP 服务

在 DHCP 服务器运行的过程中,需要 DHCP 服务的网络和 DHCP 服务器本身都有可能这样或那样的问题,需要管理员及时对 DHCP 服务器进行断开、停止、暂停、重新开始等处理,以解决问题。

要停止、启动和重新启动 DHCP 服务,可参照下面的步骤:

(1) 打开 DHCP 控制台窗口,在控制台目录树中,单击要处理的 DHCP 服务器。

(2) 要对服务器进行停止和启动等操作,可打开【操作】菜单选择【所有任务】子菜单,然后选择下列命令选项之一:

- 要启动 DHCP 服务,可单击【开始】命令;

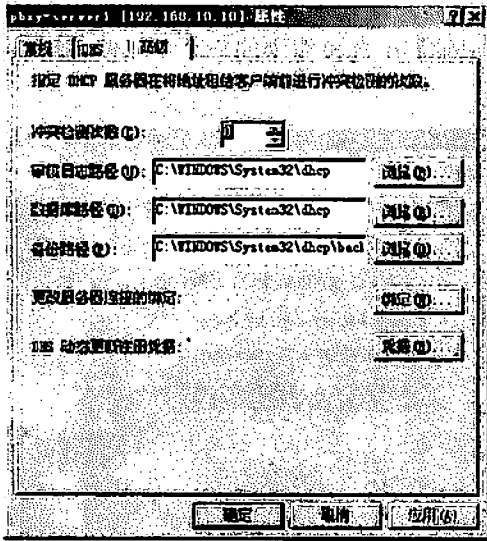


图 3.124 【高级】选项卡

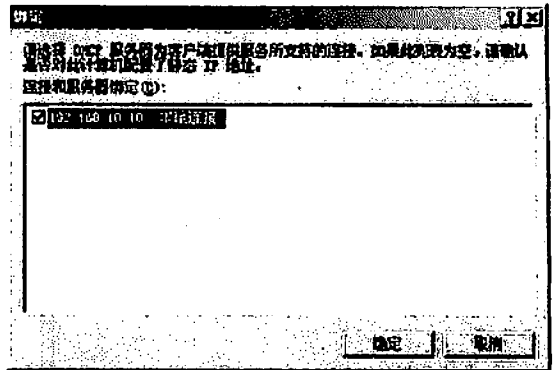


图 3.125 【绑定】对话框

- 要停止 DHCP 服务，可单击【停止】命令；
- 要中断 DHCP 服务，可单击【暂停】命令；
- 重新开始 DHCP 服务，可单击【重新开始】命令。

(3) 在暂停 DHCP 服务后，将出现【恢复】命令选项，单击该命令选项可立即继续 WINS 服务。要断开服务器的连接，可选择【操作】菜单中的【删除】命令，出现信息提示框之后单击【是】按钮即可。

### 9. 查看作用域信息

在 DHCP 控制台目录中，每一个作用域下都有 4 个子项：地址池、地址租约、保留和作用域选项。通过它们，管理员可以查看到作用域的地址范围、地址排除范围、租约和保留情况以及选项设置等。

查看作用域信息的具体操作如下：

(1) 要查看作用域的地址范围和地址排除范围，可在 DHCP 控制台目录树中展开要操作的作用域，然后单击【地址池】子节点，在详细资料窗格中就会显示出相应的内容。

(2) 对于管理员，经常需要查看 DHCP 客户机的动态 IP 地址及其他租约情况，这是通过【地址租约】节点来完成的。在控制台目录树中单击【地址租约】子节点，在详细资料窗格中就会显示出网络中所有接受 DHCP 服务的计算机的租约情况，包括客户名称、IP 地址、租约最后日期、惟一 ID 号和类型等。

(3) 要查看地址保留选项，可在控制台目录树中单击【保留】节点，在详细资料窗格中就会显示出所有的自建保留，双击要查看的保留就可查看其内容。

(4) 右击作用域节点，从弹出的快捷菜单中选择【显示统计信息】命令，可打开该作用域的统计信息显示对话框，通过该对话框可查看该作用域的地址总数、已经使用的地址数和可用地址数，如图 3.126 所示。



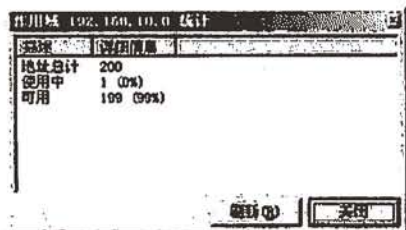


图 3.126 查看作用域地址使用情况

### 3.7.1.3 Red Flag Linux 下 DHCP 服务器配置与管理

#### 1. 启动 DHCP 配置工具

打开 DHCP 配置工具，可以采用以下方法启动 rfdhcp 工具：

- 在系统主菜单中选择【系统】|【控制面板】，打开【控制面板】，在【网络服务配置】选项卡中，双击【DHCP 配置工具】。
- 在系统主菜单中选择【管理工具】|【DHCP 配置工具】。
- 在运行命令行或 shell 提示符下直接键入 rfdhcp。

#### 2. 启动和停止 DHCP 服务：

打开 fdhcp 配置工具，在主窗口左侧的控制台树中，单击相应的 DHCH 服务器；要启动 DHCP 服务，在菜单中选择【操作】|【所有任务】|【开始】；

要停止 DHCP 服务，在菜单中选择【操作】|【所有任务】|【停止】；要重新启动 DHCP 服务，在菜单中选择【操作】|【所有任务】|【重新开始】。停止服务器之后，会出现【开始】选项并且可通过单击它再次恢复服务。

也可以在命令行终端下，通过下列命令执行这些任务：

```
#/etc/rc.d/init.d/dhcpd/start  
#/etc/rc.d/init.d/dhcpd/stop  
#/etc/rc.d/init.d/dhcpd/restart
```

#### 3. 查看 DHCP 服务器的属性

打开 rfdhcp 配置工具，在主窗口左侧的控制台树中，单击相应的 DHCP 服务器。选择菜单中的【操作】|【属性】，打开【DHCP 属性】对话框，根据需要查看或修改服务器的属性。只有网络管理员才可以选择【授权此服务器为网络上的权威服务器】。如果不能确定自己是否具有网络管理员身份，请不要选择上述选项。

#### 4. 授权 DHCP 服务器

DHCP 服务器在网络上正确配置和授权使用时，将提供有用且已计划好的管理服务。但是，当错误配置或未授权的 DHCP 服务器被引入网络时，可能会产生问题。例如，如果启动了未授权的 DHCP 服务器，它可能开始为客户机租用不正确的 IP 地址或者否认尝试更新当前地址租约的 DHCP 客户机。这些配置中的任何一个错误都可能导致启用 DHCP 的客户机产生更多的问题。例如，从未授权的服务器获取配置租约的客户机找不到有效的域控制器，致使客户机难以成功登录到网络。为避免出现这些问题，在它们为客户提供服务之

前,要在网络中验证服务器是否合法,这样就避免了由于在错误网络上运行带有不正确或正确配置的 DHCP 服务器而导致的大多数意外破坏。网络上运行的权威 DHCP 服务器将通知配置错误的 DHCP 客户机更新其配置。如果要指定一台 DHCP 服务器为权威服务器,在服务器的【属性】对话框中选择【授权此服务器为网络上的权威服务器】选项。

### 5. 管理子网

子网是对使用 DHCP 服务的子网进行的计算机管理性分组。管理员首先为每个物理子网创建子网,然后使用该子网定义由客户机使用的参数。

#### (1) 创建新子网。

① 打开 rfdhcp 工具,在主窗口左侧的控制台树中,单击相应的 DHCP 服务器、共享网络或群组。

② 在菜单中选择【操作】!【新建子网】命令,或者右击它,从弹出的快捷菜单中选择【新建子网】命令,也可以单击工具栏中的【新建子网】按钮,弹出【新建子网向导】对话框。

③ 在欢迎界面中,单击【下一步】按钮继续,出现【子网 ID 与掩码】设置界面。在【网络 ID】文本框中输入新建子网的网络标识,下面的【长度】和【子网掩码】文本框中会自动出现对应的数据。

④ 可以根据需要修改。单击【下一步】按钮规划将发放的 IP 地址范围。

⑤ 在此可以通过输入【起始 IP 地址】和【结束 IP 地址】来确定多个连续的 IP 地址范围;如果要添加一个单独的地址,则只在【起始 IP 地址】中输入数值即可。每设置一个 IP 地址范围后,单击【添加】按钮将其加入地址范围列表中。

⑥ 接着单击【下一步】按钮,设置客户端得到 IP 地址的租约时间长度。一般而言,对于一个变动性较高的局域网,就要设置较短的租约期限;而对于一个主要包含台式计算机,位置固定的网络来说,就应该设置较长的租约期限。

⑦ 单击【下一步】按钮,出现配置选项界面,这时已经设置了一个子网的基本配置。向导提示配置常用的 DHCP 选项以使用新建的子网。

⑧ 如果不打算设置这些选项,可以单击【否,我想稍后配置这些选项】按钮。这些选项可以在【子网选项】中进行设置。

⑨ 依照默认的选择【是,我想现在配置这些选项】,单击【下一步】按钮继续。

⑩ 输入为子网分配的路由器或默认网关的 IP 地址,然后单击【添加】按钮,也可以输入服务器名称。

⑪ 单击【解析】按钮让系统自动寻找其 IP 地址。如果没有预设的路由器或网关,则不必输入任何数据。

⑫ 单击【下一步】按钮继续,进入域名称和 DNS 服务器设置界面。

⑬ 输入子网上的计算机进行 DNS 名称解析时使用的父域;如果有 DNS 服务器,输入其名称或 IP 地址后单击【添加】按钮,也可以输入服务器的名称后,单击【解析】按钮让系统自动寻找其 IP 地址。

⑭ 单击【下一步】按钮,进行 WINS 服务器的相关设置,完成此步骤后,单击【下一步】按钮会出现完成新建子网向导界面。

⑮ 单击【完成】按钮，重新启动 dhcpd 服务后，客户端就可以使用这个子网中的地址了。

#### (2) 删除子网

打开 rfdhcp 配置工具，在主窗口左侧的控制台树中，单击相应的子网。选择菜单中的【操作】|【删除】命令。出现提示时，请确认是否删除该子网。无法删除共享网络中唯一的子网。

#### (3) 向子网中加入地址范围

在 rfdhcp 配置工具主窗口左侧的控制台树中，展开相应的子网，选择【地址池】选项。单击菜单中的【操作】|【新建地址范围】命令，也可以右击，并选中弹出的快捷菜单中的【新建地址范围】菜单项。在【新建地址范围】对话框中，键入要向该子网中添加的 IP 地址范围的【起始 IP 地址】和【结束 IP 地址】。如果只要添加一个单独的地址，则只输入【起始 IP 地址】即可。如果希望服务器将这个范围内的地址动态分配给 BOOTP 客户，请选中【允许 BOOTP 客户】。单击【添加】按钮，新增的地址范围将显示在主窗口右侧的地址池列表中。

#### (4) 更改或查看子网属性

在 rfdhcp 配置工具主窗口左侧的控制台树中，选择相应的子网。单击菜单中的【操作】|【属性】命令，也可以右击，并选中弹出的快捷菜单中的【属性】菜单项。打开【子网属性】对话框，可以根据需要查看或修改子网的属性。

#### (5) 查看客户机租约信息

在 rfdhcp 配置工具主窗口左侧的控制台树中，选择相应子网的【地址租约】项。在窗口右侧的详细信息列表中，可以查看客户机的租约信息。

### 6. 管理共享网络

可以通过 DHCP 配置工具创建和管理 DHCP 服务器使用共享网络可以将多个子网组合为单个管理实体。

#### (1) 创建共享网络

在 rfdhcp 配置工具主窗口左侧的控制台树中，选择相应的 DHCP 服务器或群组；单击菜单中的【操作】|【新建共享网络】命令，也可以右击，并在弹出的快捷菜单中选择【新建共享网络】菜单项，该菜单项只有在至少已经在服务器或群组中创建了一个子网，而且它目前不是共享网络或其他群组的一部分时才显示；在【新建共享网络向导】中，按提示信息完成操作。

#### (2) 删除共享网络

在 rfdhcp 配置工具主窗口左侧的控制台树中，选择相应的共享网络。单击菜单中的【操作】|【删除】命令，也可以右击，并在弹出的快捷菜单中选择【删除】命令。出现提示时，确认是否删除共享网络。删除共享网络会删除所有包含在其中的成员子网、主机、群组。如果想保留某个成员，在删除共享网络之前先将它移到服务器或其他共享网络中即可。

#### (3) 将子网添加到共享网络

在 rfdhcp 配置工具主窗口左侧的控制台树中，选择相应的子网。用鼠标将子网拖拽到希望加入的共享网络中，出现提示时，单击【是】按钮完成子网移动。



## 7. 管理主机

使用主机保留地址,可以将特定的 IP 地址分配给特定的 DHCP 客户机使用。此外也可以通过主机将一组固定的设置参数提供给指定的某些网络客户机。

### (1) 添加主机

① 在 rfdhcp 配置工具主窗口左侧的控制台树中,选择相应子网的【保留】项。

② 单击菜单中的【操作】|【新建主机】命令,也可以在右键快捷菜单中选择【新建主机】命令。

③ 在【新建主机】对话框中,输入要保留的客户机名称与 IP 地址,还有客户机的 MAC 地址。

④ 填完后单击【添加】按钮,如果不再增加其他保留地址,则单击【关闭】按钮结束。相应的主机将添加到该子网中关于保留主机,有以下几点说明请注意:可以在服务器、共享网络、群组 and 子网保留中添加主机,可以明确指定主机的 IP 地址,也可以不添加任何地址。由 DHCP 服务器动态为客户机分配地址;主机硬件一般是在相应网络连接的 DHCP 客户机媒体访问控制(MAC)地址的基础上确认的;除以太网外, DHCP 服务器也支持令牌环硬件类型,但暂不支持 FDDI 硬件; DHCP 服务器通过客户发送的惟一客户机识别码来确认客户,这个识别码由常规选项【061 惟一客户机识别码】来确定。如果这个识别码没有被定义,则需要通过对方的媒体访问控制(MAC)地址来识别主机客户。

### (2) 删除主机

打开 rfdhcp 工具,在主窗口左侧的控制台树中,选择相应的主机。单击菜单中的【操作】|【删除】命令,也可以右击,并在弹出的快捷菜单中选择【删除】项。出现提示时,请确认是否删除该主机。

### (3) 更改或查看主机属性

打开 rfdhcp 配置工具,在主窗口左侧的控制台树中,选择相应的主机。单击菜单中的【操作】|【属性】命令,也可以右击,并在弹出的快捷菜单中选择【属性】项。打开主机属性对话框,可以根据需要查看或修改主机的属性。

## 8. 管理群组

使用群组,可以将多个子网、共享网络、主机组合为单个管理实体。

对于群组成员没有定义的参数设置, DHCP 服务器会自动应用成员所属群组中的参数定义值。

### (1) 创建群组

打开 rfdhcp 配置工具,在主窗口左侧的控制台树中,选择相应的 DHCP 服务器、共享网络、子网或者群组。单击菜单中的【操作】|【新建群组】命令,也可以右击,并在弹出的快捷菜单中选择【新建群组】项。在【新建群组向导】中,按提示信息完成操作。

### (2) 增删除群组

打开 rfdhcp 配置工具,在主窗口左侧的控制台树中,选择相应的群组。

单击菜单中的【操作】|【删除】命令,也可以右击,并在弹出的快捷菜单中选择【删除】项。出现提示时,请确认是否删除该群组。



### (3) 添加成员到群组中

打开 rfdhcp 配置工具,在主窗口左侧的控制台树中,选择希望加入群组的成员节点,群组成员可以是子网、主机、共享网络或者其他的群组。用鼠标将目标成员拖拽到目的群组中,出现提示时,单击【是】移动该节点。

### 9. 设置选项

在为客户机设置了基本的 TCP/IP 配置设置(如 IP 地址、子网掩码和默认网关)之后,大多数客户机同时还需要 DHCP 服务器通过 DHCP 选项提供其他信息。

在子网、主机、共享网络以及群组中没有指派的选项将自动套用其父系节点中指派的值。

(1) 在 rfdhcp 配置工具主窗口左侧的控制台树中,展开想要配置其选项的服务器、子网、共享网络或群组,选择“xxx 选项”(xxx 代表所选的节点名称)。单击菜单中的【操作】|【配置选项】命令,也可以右击,并在弹出的快捷菜单中选择【配置选项】菜单项。打开选项设置对话框,可以根据需要查看或修改对应节点的选项。

(2) 在【可用选项】列表中,选中希望配置的对应选项;选中该选项前的复选框以激活窗口下面的【数据输入】框,键入该选项所需的必要信息。

(3) 对于任何其他希望配置的选项,请重复以上的步骤,然后单击【确定】按钮。

### 10. 使用 rfdhcp 的文件编辑器

为了使用户能够全面地配置 DHCP 服务器支持的全部功能, rfdhcp 配置工具提供了一个文件编辑器。用户可以通过这个编辑器直接对 DHCP 配置文件进行手工修改。配置工具也可以检查配置文件的语法错误。语法检查结果会显示在输出消息窗口中。

(1) 默认情况下,主窗口中不显示配置文件编辑区。在菜单中选择【查看】|【编辑器】命令,显示配置文件编辑窗口。

(2) 在编辑器窗口中对配置文件进行手工修改。单击工具栏上的“保存”按钮,保存文件,查看输出信息中的语法检查结果。如果出现语法错误,请根据提示进行修改。修改完成后,重复上面的步骤。

**注意:** 在开始手工修改配置文件后。不要在存储文件之前使用配置工具提供的其他配置功能,否则所做的修改将会被覆盖;配置文件修改并存储后,必须重新启动 DHCP 服务器才能使修改生效;输出信息中所显示的蓝色信息属于警告,红色信息属于错误;租约数据库文件不能用配置工具修改。修改租约文件可能会导致 DHCP 服务器掌握的租约信息不正确,因此在正常情况下,不对租约文件做任何修改;可以使用如下的命令来指定配置文件和租约文件的路径: rfdhcp -cf <configuration file>. -lf <lease file>; 一般情况下,请不要指定自己的租约文件。租约信息不正确会影响 DHCP 服务器的正常工作。

#### 3.7.1.4 Linux 下 DHCP 服务器配置与管理

虽然在 Windows Server 2000、Windows Server 2003 和 Red Flag Linux 环境下都可以用图形化界面来配置和管理 DHCP 服务器,考生还有必须了解在 Linux 下 DHCP 服务器配置。

### 1. DHCP 服务器软件的安装

在 Linux 下几乎采用的都是 Paul Vixie/ISC DHCPd, 来实现 DHCP 服务器端功能。用户可以访问<http://www.isc.org/isc>获得最新消息。

目前大多数 Linux 发布盘中都包含这个软件, 并以 RPM 形式提供。用户只要以 root 身份登录, 简单地用 RPM 安装就可以了。其命令格式为:

```
# rpm -ivh dhcpd-1.3.17p15.i386.rpm //1.3.17p15 为 DHCP 版本号
```

### 2. 增加主机路由

为了使 DHCP 服务器能为正确 Windows 的 DHCP 客户机服务, 需要创建一个到地址 255.255.255.255 的路由, 把这条路由命令加到/etc/rc.d/rc.local, 使得每次机器启动后自动运行。

```
#route add -host 255.255.255.255 dev eth0
```

在一些旧版 Linux 核心的系统里可能会报告错误消息:

```
255.255.255.255: Unkown host
```

可以试着加下面的条目到/etc/hosts 文件里添加:

```
255.255.255.255 dhcphost
```

再用下面的命令:

```
#route add -host dhcphost dev eth0
```

### 3. 修改配置文件

DHCP 服务默认的配置文件的/etc/dhcpd.conf, 这是一个文本文件, DHCP 服务里有一个语法分析器, 能对这个文件进行语法分析, 获得配置参数。dhcpd.conf 格式是递归下降的, 关键字大小写敏感, 可以有注释, 注释以#开头, 一直到该行结束(为了显示清晰, 下例中把注释移到行尾, 在实际配置时是不允许的)。这里给出一个简单的 dhcpd.conf 的例子, 所服务的网络为 C 类保留网络 192.168.1.0。

#dhcpd.conf 配置实例

subnet 192.168.1.0 netmask 255.255.255.0 {	# 子网声明和掩码
range 192.168.1.10 192.168.1.100;	# 范围
range 192.168.1.150 192.168.1.200;	# 范围
#全局参数设置	
default-lease-time 28800;	# 默认租约时间
max-lease-time 43200;	# 最大租约时间
option subnet-mask 255.255.255.0;	# 子网掩码选项
option broadcast-address 192.168.1.255;	# 广播地址
option routers 192.168.1.1;	# 路由器地址
option domain-name-servers 192.168.1.1;	# DNS 地址
option domain-name "netreslab.org";	# 域名
}	

这段配置文件将允许 DHCP 服务器分配两段地址范围给 DHCP 客户, 192.168.1.10~192.168.1.100 和 192.168.1.150~192.168.1.200; 如果 DHCP 客户在申请租约时不请求一个特定租约失效时间, 则以 default-lease-time(28800 秒)为租约时间, 如果有请求一个特定的租约失效时间, 则采用 max-lease-time(432000 秒)。

服务器发送下面的参数给 DHCP 客户机: 子网掩码是 255.255.255.0, 广播地址是 192.168.1.255, 默认网关是 192.168.1.1, DNS 是 192.168.1.1。

如果要为一台叫做 hotdog 的机器指定固定的 IP 地址, 可以在 dhcpd.conf 文件中增加一条。

```
host hotdog {                                # 为 hotdog 指定固定的 IP 地址
hardware ethernet 08:00:00:4c:58:23;        # hotdog 上网卡的硬件地址
fixed-address 192.168.1.210;                # 固定 IP
}
```

#### 4. dhcpd.leases 文件

dhcpd.leases 是 DHCP 客户租约的数据库文件, 默认目录为 /var/state/dhcp/, 文件包含租约声明。每次一个租约被获取、更新或释放, 它的新值就被记录到文件的末尾。在 dhcpd 第一次安装后, 并不会生成这个文件。但 dhcpd 的运行需要这个文件, 所以可以建立一个空的文件:

```
#touch /var/state/dhcp/dhcpd.leases
```

dhcpd 记录这个文件的格式是:

```
lease ip-address { statements... }
```

每个记录包含一个提供给客户的 IP 地址, 在花括号里的语句包含一些租约信息。具体的租约信息因客户发出不同的 DHCP 请求而稍有差别。

如果我们启动一台 Windows 98 机器, Windows 98 的网络配置的 TCP/IP 选项里指定自动获得 IP 地址, 也就是启用 Windows 98 里的 DHCP 客户程序, 这台机器的主机名为 ONE。在 Windows 98 机器获得租约后, dhcpd 会在 dhcp.leases 里建一条记录:

```
lease 192.168.1.154 {
starts 1 2000/05/15 13:36:42;
ends 1 2000/05/15 21:36:42;
hardware ethernet 00:00:21:4e:3f:58;
uid 01:00:00:21:4e:3f:58;
client-hostname one;
}
```

要注意的是 dhcpd.leases 的时间记录采用 GMT 时间, 而不是本地时区的时间。要查看本机的 GMT 时间可以用 “date -u” 命令。

#### 5. 运行 DHCP 服务

用户可以使用 dhcpd 守护程序来启动、重新启动、停止 DHCP 服务。

启动 DHCP 服务的命令是:

```
/etc/rc.d/init.d/dhcpd start.
```

这样启动后, dhcpd 是启动在 eth0 上, 如果 dhcpd 上的服务器还有另外一块网卡 eth1, 想在 eth1 上启动 DHCP 服务, 命令是:

```
#/usr/sbin/dhcpd eth1
```

如果在修改配置文件 dhcpd.conf 后, 希望立即生效, 可重新启动 DHCP 服务, 其命令是:

```
#/etc/rc.d/init.d/dhcpd restart
```

如果希望暂时停止 DHCP 服务, 其命令是:

```
#/etc/rc.d/init.d/dhcpd stop
```

设定 DHCP 服务在计算机启动时自动启动或不启动, 可以使用 ntsysv 命令将它加到引导程序中, 也可以通过 chkconfig 命令来设定, 该命令格式是:

```
chkconfig [--level <运行级>] <名字> [on|off]
```

例如我们希望在运行级别 3、5 启动计算机时启动 DHCP 服务, 则命令为:

```
#chkconfig --level 3,5 dhcpd on
```

再如我们希望在运行级别 2 启动计算机时不启动 DHCP 服务, 则命令为:

```
#chkconfig --level 2 dhcpd off
```

如果希望在任何运行级别下启动时都不启动 DHCP 服务, 只需将 “[--level <运行级>]” 不设定就可以了, 即:

```
#chkconfig dhcpd on  
#chkconfig dhcpd off
```

## 6. dhcpd.conf 详解

### (1) dhcpd.conf 概述

前面说过, dhcpd.conf 是个递归下降格式的配置文件的, 有点像 C 语言的源程序风格, 由参数和声明两大类语句构成, 参数类语句主要告诉 DHCPd 网络参数, 如租约的时间、网关、DNS 等, 而声明语句则是描述网络的拓扑, 用来表明网络上的客户和要提供给客户的 IP 地址以及提供一个参数组给一组声明等。

描述网络拓扑的声明语句有 shared-network 和 subnet 声明。如果要给一个子网里的客户动态指定 IP 地址, 那么在 subnet 声明里必须有一个 range 声明, 说明地址范围。如果要给 DHCP 客户静态指定 IP 地址, 那么每个这样客户都要有一个 host 声明。对于每个要提供服务的与 DHCP 服务器连接的子网, 都要有一个 subnet 声明, 即使这是个没有 IP 地址要动态分配的子网也需要有。

### (2) 语句参考

因为 DHCPd 的语句很多, 不可能一一列出, 这里给出最常用和最重要的语句。



### ① 声明类语句

#### ● share-network 语句

语法:

```
shared-network name {  
    [ 参数 ]  
    [ 声明 ]  
}
```

说明:

**share-network** 用于告知 DHCP 服务器某些 IP 子网其实是共享同一个物理网络。任何一个在共享物理网络里的子网都必须声明在 **share-network** 语句里。当属于其子网里的客户启动时, 将获得在 **share-network** 语句里指定参数, 除非这些参数被 **subnet** 或 **host** 里的参数覆盖。用 **share-network** 是一种权宜之计, 例如某公司用 B 类网络 145.252, 公司里的部门 A 被划在子网 145.252.1.0 里, 子网掩码为 255.255.255.0, 这里子网号为 8 位, 主机号也为 8 位, 但如果部门 A 急速增长, 超过了 254 个节点, 而物理网络还来不及增加, 就要在原来这个物理网络上跑两个 8 位掩码的子网, 而这两个子网其实是在同一个物理网络上, **share-network** 语句形式如下:

```
shared-network share1 {  
    subnet 145.252.1.0 netmask 255.255.255.0 {  
        range 145.252.1.10 145.252.1.253;  
    }  
    subnet 145.252.2.0 netmask 255.255.255.0 {  
        range 145.252.2.10 145.252.2.253;  
    }  
}
```

这里的 **share1** 是个共享网络名。

#### ● subnet 语句

语法:

```
subnet subnet-number netmask netmask {  
    [ 参数 ]  
    [ 声明 ]  
}
```

说明:

**subnet** 语句用于提供足够的信息来阐明一个 IP 地址是否属于该子网。也可以提供指定的子网参数和指明那些属于该子网的 IP 地址可以动态分配给客户, 这些 IP 地址必须在 **range** 声明里指定。**subnet-number** 可以是 IP 地址或能被解析到这个子网的子网号的域名。**netmask** 可以是 IP 地址或能被解析到这个子网的掩码的域名。

**range** 语句

语法:

```
range [ dynamic-bootp ] low-address [ high-address];
```

说明:

对于任何一个有动态分配 IP 地址的 subnet 语句,至少要有一个 range 语句,用来指明要分配的 IP 地址的范围。如果只指定一个要分配的 IP 地址,那么高地址部分可以省略。

- host 语句

语法:

```
host hostname {  
  [ 参数 ]  
  [ 声明 ]  
}
```

说明:

host 语句的作用是为特定的客户机提供网络信息。

- group 语句

语法:

```
group {  
  [ 参数 ]  
  [ 声明 ]  
}
```

说明:

group 语句的作用是给一组声明提供参数。

- allow 和 deny 语句

allow 和 deny 语句用来控制 dhcpd 对客户请求。

```
allow unknown-clients;  
deny unknown-clients;
```

allow unknown-clients 允许 dhcpd 可以动态分配 IP 给未知的客户,而 deny unknown-clients 则不允许。默认为允许。

- bootp 关键字

```
allow bootp;  
deny bootp;
```

指明 dhcpd 是否响应 bootp 查询,默认为允许。

② 参数类语句:

- default-lease-time 语句

语法:

```
default-lease-time time;
```

说明:

指定默认租约时间,这里的 time 是以秒为单位的。它用来指定 DHCP 客户机在租约 IP 地址后什么时间需要向 DHCP 服务器重新申请 IP 地址租约。

- max-lease-time 语句

语法:

```
max-lease-time time;
```

说明:

最大的租约时间。如果 DHCP 在请求租约时间时有发出特定的租约失效时间的请求, 则用最大租约时间。

- hardware 语句

语法:

```
hardware hardware-type hardware-address;
```

说明:

指明物理硬件接口类型和硬件地址。硬件地址由 6 个 8 位组构成, 每个 8 位组以 “:” 隔开。如 00:00:E8:1B:54:97

- server-name 语句

语法:

```
server-name name;
```

说明:

用于告知客户服务器的名称。

- fixed-address 语句

语法:

```
fixed-address address [, address ... ];
```

说明:

fixed-address 语句用于指定一个或多个 IP 地址给一个 DHCP 客户。只能出现在 host 声明里。

### ③ 选项类语句

选项类语句以 option 开头, 后面跟一个选项名, 选项名后是选项数据, 选项非常多, 这里列出一些常用的选项供参考:

- option subnet-mask < subnet-netmask>;

指明子网掩码。

- option routers ip-address[, ip-address];

指明在子网内的默认网关(即路由器)的地址, 可以有多个。

- option time-servers ip-address[, ip-address...];

指明时间服务器的地址。

- option domain-name-servers ip-address[, ip-address...];

指明 DNS 的地址。

- option host-name string;

给客户指定主机名, string 为字符串。

- option domain-name string;

指明域名。

- option interface-mtu mtu;

指明网络界面的 mtu, 这里 mtu 为正整数。

例 option interface-mtu 1500;

- option broadcast-address ip-address;

指定广播地址。

### 3.7.2 典型例题分析

例 1 阅读以下说明, 回答问题 1~5, 将答案填入对应的解答栏内。

【说明】

某公司在国际网互联中心申请了 210.45.12.0/24 一个 C 类的 IP 地址, 并申请了一个域名为 abc.com.cn。该公司没有划分子网, 使用一台 Cisco 2610 路由器接入互联网, 其接入内部局域网的 IP 地址是 210.45.12.99, 并一台 DNS 服务器(210.45.12.10)、有一台该 Web 服务器(210.45.12.100), 一台 FTP 服务器(210.45.12.101)和一台 MAIL 服务器(210.45.12.102)。

原来该公司采用手工分配 IP 地址, 现要改用 DHCP 自动分配 IP 地址, 拟使用一台安装有 Windows Server 2003 的 PC 服务器作为 DHCP 服务器, 它的 IP 地址为 210.45.12.103。若你是该公司的网络管理员, 需要配置这台 DHCP 服务器。假设该公司不会有新服务器, 把所有的地址都动态地分配给客户机。

【问题 1】该作用域的 IP 地址范围是什么? 子网掩码是多少?

【问题 2】排除范围是什么?

【问题 3】默认网关是什么?

【问题 4】域名是什么? 域名服务器 IP 地址是什么?

【问题 5】该公司销售部有一台 PC 机, 由于其工作性质决定了必须要有一个固定 IP 地址, 你如何给它分配一个固定 IP 地址? (写出两种方案)

分析: 该题主要考查考生对 Windows Server 2003 下 DHCP 服务器配置的掌握情况。

问题 1: 该公司的网络地址是 210.45.12.0/24, 其可用范围是 210.45.12.1~210.45.12.254, 210.45.12.0 用来定义子网(子网地址), 而 210.45.12.255 用于网内广播(广播地址)。又由于该公司不会有新服务器, 把所有的地址都动态地分配给客户机, 所以该作用域的 IP 地址范围是 210.45.12.1~210.45.12.254。该公司没有划分子网, 必须用 C 类的 IP 地址默认子网掩码作为子网掩码, 即 255.255.255.0。

问题 2: 在设置 DHCP 服务作用域时, 必须把路由器、服务器(包括 DHCP 服务器本身地址)排除在外。根据说明的要求, 必须把 210.45.12.10 和 210.45.12.99~210.45.12.103 排除在外。

问题 3: 默认网关地址指的是路由器的地址, 即 Cisco 2610 路由器接入内部局域网的 IP 地址是 210.45.12.99。

问题 4: 域名和域名服务器都是 DHCP 服务选项, 其目的是告诉客户机如何设置域名和域名服务器。因此, 域名为 abc.com.cn, 域名服务器 IP 地址是 210.45.12.10。

问题 5: 要给一台主机分配一个固定的 IP 地址, 通常有两种做法。一种是把要分配给



该主机的 IP 地址加入排除范围之内,第二种办法是新建保留特定的地址,这是要输入保留名称、保留 IP 地址和该主机网卡的 MAC 地址。

答案:

【问题 1】该作用域的 IP 地址范围是 210.45.12.1~210.45.12.254,子网掩码为 255.255.255.0。

【问题 2】210.45.12.10、210.45.12.99~210.45.12.103。

【问题 3】210.45.12.99。

【问题 4】域名为 abc.com.cn,域名服务器 IP 地址是 210.45.12.10。

【问题 5】第一种方法是把要分配给该主机的 IP 地址加入排除范围之内,第二种办法是新建保留特定的地址,这是要输入保留名称、保留 IP 地址和该主机网卡的 MAC 地址。

例 2 阅读以下说明,回答问题 1~6,将解答填入答题纸对应的解答栏内。(2004 年下半年网络管理员下午试题四)

【说明】

在 Linux 下安装配置 DHCP 服务,DHCP 服务程序/usr/sbin/dhcpd 需要读取配置文件/etc/dhcpd.conf,以下是一个 DHCP 配置文件的主要内容:

```
subnet 200.117.207.0 netmask 255.255.255.0{
range 200.117.207.10 200.117.207.100;
range 200.117.207.110 200.117.207.200;
default-lease-time 86400;
max-lease-time 604800;
option subnet-mask 255.255.255.0;
option routers 200.117.207.1;
option domain-name "myuniversity.edu.cn";
option broadcast-address 200.117.207.255;
option domain-name-servers 200.117.207.3;
}
```

【问题 1】此配置允许 DHCP 服务器分配给客户的地址范围是什么?

【问题 2】如果客户机希望连续使用得到的 IP 地址,那么它在租用 IP 地址后每隔多少秒必须发送一次租用续约请求?

【问题 3】DHCP 服务器发送给客户机的信息中子网掩码是什么?DNS 服务器的地址是什么?路由器的地址是什么?

【问题 4】#sbin/chkconfig -level 3 dhcpd on 命令的作用是什么?

【问题 5】配置完毕后,可以用什么命令重新启动操作系统?

【问题 6】Red Flag Linux 4.0 提供了 DHCP 配置工具,在命令行或 Shell 提示符下应输入什么命令启动该工具?

分析:该题主要考查考生对 Linux 下 DHCP 服务器配置的掌握情况。

DHCP 服务默认的配置文件是/etc/dhcpd.conf,这是一个文本文件,DHCP 服务根据该文件获得配置参数。

dhcpd.conf 由参数和声明两大类语句构成。参数类语句主要告诉 DHCPd 网络参数,如

租约的时间、网关、DNS 等,而声明语句则是描述网络的拓扑,用来表明网络上的客户、要提供给客户的 IP 地址、提供一个参数组给一组声明等。

问题 1: 在 `/etc/dhcpd.conf` 文件中, `range` 语句用来指明要分配的 IP 地址的范围。在该例中,共有两条 `range` 语句,分别指定两段 IP 地址空间,因此 DHCP 服务器分配给客户的地址范围是 200.117.207.10~200.117.207.100 和 200.117.207.110~200.117.207.200。

问题 2: 在 Linux 下配置 DHCP 服务器时一般要配置两个时间,一个缺省租约时间,它用来指定 DHCP 客户机在租约地址后什么时间需要向 DHCP 服务器重新申请 IP 地址租约,缺省租约时间使用 `default-lease-time` 语句来定义的,另一个是最大的租约时间,它用来指定 DHCP 客户机在租用续约请求遭到 DHCP 服务器拒绝时,什么时间必须放弃 IP 地址租约,最大的租约时间使用 `max-lease-time` 语句来定义的。考生必须区分这两种的区别,这两个语句的时间单位均为秒。因此如果一客户机希望连续使用得到的 IP 地址,那么它在租用 IP 地址后每隔 86400 秒必须发送一次租用续约请求,即有 `default-lease-time` 语句指定的时间。

问题 3: DHCP 客户机在获得 IP 地址租约的同时,也获得其他的配置参数(如子网掩码、默认网关、DNS 服务器、域名等),这些参数通常是由 `option` 语句来定义,`option subnet-mask` 用来指明子网掩码,`option routers` 用来指明在客户子网内的默认网关(即路由器)地址,`option domain-name` 用来指明域名,`option domain-name-servers` 用来指明 DNS 服务器地址。DHCP 服务器发送给客户机的信息中子网掩码是 255.255.255.0, DNS 服务器的地址是 200.117.207.3,那么路由器的地址是 200.117.207.1。

问题 4: `chkconfig` 命令用于修改 Linux 操作系统开机时在每一个运行等级(Run Level)中要自动启动和关闭的程序。该命令格式是:

```
chkconfig [--level <运行级>] <名字> [on|off]
```

例如,我们希望在运行级别 3、5 启动计算机时启动 DHCP 服务,则命令为:

```
#chkconfig --level 35 dhcpd on
```

再如,我们希望在运行级别 2 启动计算机时不启动 DHCP 服务,则命令为:

```
#chkconfig --level 2 dhcpd off
```

因此,问题 4 的命令作用是设置当操作系统按运行级 3 启动时自动启动 DHCP 服务。

问题 5: 重新启动 Linux 操作系统有如下两种命令:第一种命令是 `reboot`,第二个命令是 `shutdown -r`。

问题 6: 在 Red Flag Linux 下启动 DHCP 配置工具通常有三种办法:一种系统主菜单中选择【系统】|【控制面板】,打开【控制面板】窗口,在【网络服务配置】选项卡中,双击【DHCP 配置工具】;第二种在系统主菜单中选择【管理工具】|【DHCP 配置工具】;第三种方法是在运行命令行或 shell 提示符下直接键入 `rfdhcp`。方法三就是本问题的答案。

答案:

【问题 1】200.117.207.10~200.117.207.100 和 200.117.207.110~200.117.207.200

【问题 2】86400

【问题 3】子网掩码: 255.255.255.0; DNS 服务器的地址: 200.117.207.3; 路由器的地

址: 200.117.207.1

【问题4】设置当操作系统按运行级3启动时自动启动DHCP服务

【问题5】reboot(或 shutdown -r)

【问题6】rfdhcp

例3 阅读以下说明,回答问题1~6,将答案填入对应的答案栏内。

【说明】

某公司在国际网互联中心申请了210.45.12.0/24一个C类的IP地址,并申请了一个域名为abc.com.cn,其DNS服务器的地址是210.45.12.103。该公司没有划分子网,使用一台Cisco 2610路由器接入互联网,其接入内部局域网的IP地址是210.45.12.1。

原来该公司采用手工分配IP地址,现要改用DHCP自动分配IP地址,拟使用一台安装有RedHat Linux的PC服务器作为DHCP服务器。该公司准备把210.45.12.20~210.45.12.120和210.45.12.150~210.45.12.250这两块地址用于动态分配给客户机,其他地址用作服务器IP或保留下来以便网络扩充。下面是DHCP服务配置文件/etc/dhcpd.conf的主要内容:

```
subnet 210.45.12.0 netmask 255.255.255.0 {
    _____ (1) _____;
    range 210.45.12.150      210.45.12.250;
    default-lease-time 86400;
    max-lease-time 604800;
    option subnet-mask 255.255.255.0;
    option routers _____ (2) _____;
    option domain-name " _____ (3) _____ ";
    option broadcast-address 200.117.207.255;
    option domain-name-servers _____ (4) _____;
    host mypc {
        hardware ethernet 00:0a:e6:b2:2f:5b;
        fixed-address 210.45.12.215;
    }
}
```

【问题1】(1)处应当填写什么内容?

【问题2】(2)处应当填写什么内容?

【问题3】(3)处应当填写什么内容?

【问题4】(4)处应当填写什么内容?

【问题5】文件/etc/dhcpd.conf中阴影部分的含义是什么?

【问题6】文件/var/state/dhcp/dhcpd.leases在DHCP中起什么作用?

分析:该题主要考查考生对Linux下DHCP服务器配置的掌握情况。

问题1:该公司要把210.45.12.20~210.45.12.120和210.45.12.150~210.45.12.250这两块地址用于动态地分配给客户机。因此在该文件中必须要进行声明,用来指明要分配的IP地址的范围,其语句是range语句。文件中已经对210.45.12.150~210.45.12.250地址块进行了

声明, (1)应对 210.45.12.20~210.45.12.120 地址块进行声明, 因此, 应填写 “range 210.45.12.20 210.45.12.120”。

问题 2: option 语句主要指明一些网络参数, 其中 “option routers ip-address[, ip-address]” 命令来指明在客户子网内的默认网关地址。 (2)处应当填写该地址, 即路由器接入内部局域网端口的 IP 地址, 因此, 应填写 “210.45.12.1”。

问题 3: option domain-name 语句用于指定域名, 因此(3)处应填写 “abc.com.cn”。

问题 4: option domain-name-servers 语句用于指定 DNS 服务器的 IP 地址, 因此(3)处应填写 “210.45.12.103”。

问题 5: host 语句的作用是为特定的客户机提供网络信息。文件/etc/dhcpd.conf 中阴影部分说明了把 210.45.12.215 固定地分配给 mypc 这台主机, 这台主机网卡的 MAC 地址是 00:0a:e6:b2:2f:5b。

问题 6: dhcpd.leases 是 DHCP 客户租约的数据库文件, 默认目录在/var/state/dhcp/, 文件包含租约声明, 每次有一个租约被获取、更新或释放, 它的新值就被记录到文件的末尾。

答案:

【问题 1】 range 210.45.12.20 210.45.12.120

【问题 2】 210.45.12.1

【问题 3】 abc.com.cn

【问题 4】 210.45.12.103

【问题 5】把 210.45.12.215 固定地分配给 mypc 这台主机, 这台主机网卡的 MAC 地址是 00:0a:e6:b2:2f:5b。

【问题 6】它是 DHCP 客户租约的数据库文件, 存放 IP 地址租约信息。

### 3.7.3 同步练习

1. 通过下列哪种协议可以在网络中动态地获得 IP 地址?  
A. DHCP                  B. SNMP                  C. PPP                  D. UDP
2. DHCP 的工作原理是什么?
3. DHCP 服务器能为客户机提供哪些参数?
4. 在 Windows 2003 域结构中, 在配置 DHCP 作用域前必须要进行授权, 其目的是什么?
5. 在 Red Flag Linux 中如何启动 DHCP 服务? 请说出两种方式。
6. 在 Red Flag Linux 的 DHCP 配置工具中编辑器的功能是什么?
7. 阅读以下说明, 回答问题 1~5, 将答案填入对应的答案栏内。

【说明】

在 Linux 下安装配置 DHCP 服务, DHCP 服务程序/usr/sbin/dhcpd 需要读取配置文件/etc/dhcpd.conf, 以下是一个 DHCP 配置文件的主要内容:

```
subnet 210.45.12.0 netmask 255.255.255.0 {  
range 210.45.12.40 210.45.12.120;
```



```
range 210.45.12.150 210.45.12.225;
default-lease-time 86400;
max-lease-time 604800;
option subnet-mask 255.255.255.0;
option routers 210.45.12.254;
option domain-name "xyz.com.cn";
option broadcast-address 210.45.12.255;
option domain-name-servers 210.45.12.10;
}
```

【问题 1】此配置允许 DHCP 服务器给客户的地址范围是什么？

【问题 2】如果客户机连续请求继续租约 IP 地址都失败，那么它在租用 IP 地址最长时间是多少秒？

【问题 3】DHCP 服务器发送给客户机的信息中子网掩码是什么？DNS 服务器的地址是什么？路由器的地址是什么？

【问题 4】配置完毕后，可以用什么命令启动 DHCP 服务？（不重新启动计算机）

【问题 5】在 Linux 下配置 DHCP 服务，必须要创建一个名为 dhcpd.leases 的 DHCP 客户租约数据库文件，创建的命令是什么？

### 3.7.4 同步练习参考答案

1. A

2. 略

3. 参数主要有 IP 地址、子网掩码、默认网关、域名、DNS 服务器 IP 地址等基本的网络配置参数。若使用 Windows Server 2003 还可以指定 WINS 服务器 IP 地址。

4. 防止非法的 DHCP 服务器分配错误 IP 地址和配置参数而引起网络故障。

5. 第一种方法是在命令行或 Shell 提示符应输入 `#/etc/rc.d/init.d/dhcpd/start` 命令；第二种方法是启动 DHCP 配置工具，在主窗口左侧的控制台中，单击相应的 DHCP 服务器，在菜单中选择【操作】|【所有任务】|【开始】。

6. DHCP 配置工具中编辑器的功能使得用户可以手工修改 DHCP 配置文件。

7.

【问题 1】210.45.12.40~210.45.12.120 和 210.45.12.150~210.45.12.225

【问题 2】604800

【问题 3】子网掩码是 255.255.255.0，DNS 服务器的地址是 210.45.12.10，路由器的地址是 210.45.12.254

【问题 4】`/etc/rc.d/init.d/dhcpd restart`

【问题 5】`# touch /var/state/dhcp/dhcpd.leases`

## 3.8 本章小结

本章主要介绍局域网服务器各种应用服务的配置，包括 IP 地址、子网掩码的规划配置；

DNS 服务器的规划、设置和维护；电子邮件服务器的规划、设置和维护；FTP 服务器的规划、设置和维护；代理服务器的规划、设置和维护；DHCP 服务器的安装与设置。在每一种服务都分别介绍了在 Windows Server 2003、Red Flag Linux 和 Linux(以 Red Hat Linux 为例)下配置。

由于教材在应用服务器的配置方面介绍不够全面，有的只介绍了在 Red Flag Linux 下进行配置，有的只介绍了在 Windows Server 2003 下进行配置，对 Linux 环境下如何通过配置文件来配置服务器都没有涉及，根据大纲要求，本章对上述三种环境下各种应用服务配置都作了详细的讲解，以便考生复习。对 IP 地址、子网掩码的规划配置教材也没涉及，本章详细作了阐述。另外，Apache 服务器的知识虽然大纲中并没规定需要掌握，但教材中介绍了在 Red Flag Linux 下配置的情况，这里补充了在 Linux 环境下通过配置文件来配置 Apache 服务器，以便考生复习。本章知识点非常多，也是下午考试的重点之一。由于对应用服务器的配置是一个实践性很强的工作，考生在复习本章时，尽可能亲手配置一下这些服务，这样印象会更深，学习起来能够理论联系实际，能更有效地掌握本章的知识。同时要注意配合《网络管理员考试同步辅导(计算机与网络基础知识篇)》第五章介绍的各种服务器基础知识一起学习。

根据对 2004 年下半年的考题分析，由于 Windows Server 2003 和 Red Flag Linux 都是使用图形化配置工具完成服务器配置，在出题上时考题难度很难把握，因此考生应把重点放在 Linux 环境下通过配置文件来配置这些服务，重点掌握各种服务的在 Linux 环境下配置文件的结构、语法和含义。

本章的每小节中组织了大量的针对水平考试的典型例题分析和同步训练，这些题目基本上涵盖了大纲规定的知识要点。

## 3.9 达标训练题及参考答案

### 3.9.1 达标训练题

1. 阅读以下说明，回答问题 1~3，将答案填入对应的答案栏内。

**【说明】**

某单位有一个网络，其中有一台主机的 IP 地址是 190.190.247.134。请回答以下问题：

**【问题 1】**这个地址是一个什么类型的地址？不划分子网时，其网络地址是多少？广播地址是什么？

**【问题 2】**它的默认子网掩码是什么？

**【问题 3】**若子网掩码是 255.255.240.0，则这台主机所在的子网地址是什么？该子网的广播地址是什么？这个 IP 地址所在的子网的主机 IP 范围是什么？

2. 阅读以下说明，回答问题 1~4，将解答填入对应的答案栏内。

**【说明】**

某公司申请了一个 C 类地址 196.102.56.0，公司有生产部门、市场部门、财务部门、人事部门、技术部门和经理办公室，每个部门都需要划分为单独的网络，即需要划分至少

5 个子网，每个子网至少支持 24 台主机。(使用固定子网掩码)

【问题 1】将子网掩码设置什么？

【问题 2】每个子网有多少主机地址？

【问题 3】196.102.56.197 所在子网的网络地址是什么？

【问题 4】196.102.56.197 所在子网的广播地址是什么？

3. 阅读以下说明，回答问题 1~4，将解答填入对应的答案栏内。

【说明】

某一小型公司从 ISP 申请了一个 Internet 出口，ISP 给该公司提供了 5 个 IP 地址，分别是 222.34.109.66~222.34.109.70，ISP 给该公司提供的路由器地址是 222.34.109.65。

【问题 1】由于 ISP 忘记告诉子网掩码，你认为最有可能的子网掩码是什么？

【问题 2】这个子网的子网地址是什么？

【问题 3】这个子网有广播地址是什么？

4. 阅读以下说明，回答问题 1~3，将答案填入对应的答案栏内。

【说明】

某公司被分配了一个 C 类地址 200.100.50.0，根据需要，该公司将网络划分成若干个子网，其中：有 4 个子网，每个子网最多有主机 30 台；有 3 个子网，每个子网最多有主机 5 台；另外还有 9 个点点到点串行链路。

【问题 1】请为该网络进行子网分割，至少有 3 个不同变长的子网掩码，并画出子网划分示意图。注意：该单位的路由器不支持全 0 和全 1 子网。

【问题 2】请列出你所分配的网络地址。

【问题 3】为该网络分配点到点串行链路地址。

5. IP 地址由 32 个二进制位构成，其组成结构为 IP 地址：网络地址+主机地址。分为五类(A 类至 E 类)，其中提供作为组播(Multicast)地址的是 (1)，A 类地址用前 8 位作为网络地址，后 24 位作为主机地址，A 类网络个数为 (2)；B 类地址用前 16 位作为网络地址，后 16 位作为主机地址，可以实际分配的属于 B 类全部 IP 地址共有 (3) 个。采取子网划分后，IP 地址的组成结构为 (4)，子网划分导致实际可分配 IP 地址数目减少，一个 C 类网络采用主机地址的前两位进行子网划分时，减少的地址数目为 (5)。

(1) A. A 类地址      B. C 类地址      C. D 类地址      D. E 类地址

(2) A. 127      B. 126      C. 255      D. 128

(3) A.  $16384 \times 65536$       B.  $16384 \times 65534$   
C.  $16382 \times 65534$       D.  $16382 \times 65536$

(4) A. IP 地址：网络地址+子网地址+主机地址  
B. IP 地址：网络地址+子网络接口地址+主机地址  
C. IP 地址：网络地址+主机地址+子网络接口地址  
D. IP 地址：网络地址+主机地址+子网地址

(5) A. 6      B. 8

6. 在 Internet 中，IP 地址 168.147.52.38 属于 (1) 地址，该地址的二进制表示是 (2)。如果 IP 地址为 127.0.0.1，那么它通常表示 (3)。从 IP 地址空间划分来看，B 类地址最多可包含 (4) 个子网，每个 B 类网络最多可包含 (5) 个主机地址。

- (1) A. A 类                      B. B 类                      C. C 类                      D. D 类
- (2) A. 10011000.10010011.00110100.00100110  
 B. 10101000.10010100.00110100.00100110  
 C. 10101000.10010011.00110100.00100110  
 D. 10101000.10010011.00110110.00100110
- (3) A. 实现本机回送功能的地址                      B. A 类广播地址  
 C. 无效地址                      D. B 类广播地址
- (4) A.  $2^{14}-2$                       B.  $2^{14}-1$                       C.  $2^{14}$                       D.  $2^{16}$
- (5) A.  $2^{14}-2$                       B.  $2^{14}$                       C.  $2^{16}-2$                       D.  $2^{16}$

7. 采用可变长子网掩码技术可以把大的网络分成较小的子网, 例如把子网掩码为 255.255.0.0 的网络 40.15.0.0 分为两个子网, 假设第一个子网为 40.15.0.0/17, 则第二个子网为 (1)。假设用户 X1 有 2000 台主机, 则至少应给他分配 (2) 个 C 类网络, 如果分配给用户 X1 的网络号为 196.25.64.0, 则指定给 X1 的超网掩码为 (3); 假设给用户 X2 分配的 C 类网络号为 196.25.16.0~196.25.31.0, 则 X2 的超网掩码应为 (4); 如果路由器收到一个目标地址为 11000100. 00011001. 01000011. 00100001 的数据报, 则该数据报应送给 (5) 用户。

- (1) A. 40.15.1.0/17                      B. 40.15.2.0/17  
 C. 40.15.100.0/17                      D. 40.15.128.0/17
- (2) A. 4                      B. 8                      C. 10                      D. 16
- (3) A. 255.255.255.0                      B. 255.255.250.0                      C. 255.255.248.0                      D. 255.255.240.0
- (4) A. 255.255.255.0                      B. 255.255.250.0                      C. 255.255.248.0                      D. 255.255.240.0
- (5) A. X1                      B. X2                      C. X1 和 X2                      D. 非 X1 且非 X2

8. IPv4 地址可以划分为{网络号, 主机号}两部分。在下面的地址标记中, 用 0 表示所有位为 0, 用 -1 表示所有位为 1。以下选项中, (1) 不能作为目标地址, (2) 不能作为源地址, (3) 只能用于本机测试, (4) 只能用于内部网络。IPv6 使用了更大的地址空间, 每个地址占有 128 位, 为方便网络管理人员阅读和管理, 采用 (5) 进制数加冒号的表示方法。

- (1) A. {0, 0}                      B. {127, 主机号}                      C. {10, 主机号}                      D. {网络号, -1}
- (2) A. {0, 0}                      B. {127, 主机号}                      C. {10, 主机号}                      D. {网络号, -1}
- (3) A. {0, 0}                      B. {127, 主机号}                      C. {10, 主机号}                      D. {192, -1}
- (4) A. {0, 0}                      B. {128, 主机号}                      C. {10, 主机号}                      D. {168, -1}
- (5) A. 十六                      B. 十                      C. 八                      D. 二

9. 阅读以下说明, 回答问题 1~6, 将解答填入对应的答案栏内。

【说明】

某公司的域名为 xyz.com.cn, 所使用的网络地址为 199.168.10.0/24, 共有两台服务器, 一台的 IP 地址是 199.168.10.201, 名字是 s1, 它用作域名服务器, 另一台 IP 地址是 199.168.10.201, 名字是 s2, 它用作 WWW 服务器。下面是从该公司 s1 主机中的得到的三个文件的内容。

/etc/named.conf 文件的内容:



```

options {
    directory "/var/named";
};

zone "." IN {
    type hint;
    file "named.ca";
};

zone "0.0.127.in-addr.arpa" IN {
    type master;
    file "named.local";
    allow-update { none; };
};

zone " xyz.com.cn " IN {
    type master;
    file " named.hosts";
    allow-update { none; };
};

zone " _____ (1) _____ " IN {
    type master;
    file "named.rev";
    allow-update { none; };
};

```

/var/named/named.hosts 文件的内容:

```

$TTL 86400
@      IN  SOA      s1.xyz.com.cn. root.xyz.com.cn. (
                                2001110600 ; serial
                                28800 ; refresh
                                14400 ; retry
                                3600000 ; expire
                                86400 ; minimum
                                )
      IN  NS   s1.xyz.com.cn.
      IN  MX   10 s1.xyz.com.cn.
localhost. IN  A   127.0.0.1
s1      IN  A   199.168.10.201
s2      IN  A   199.168.10.202
www     IN  CNAME  s1

```

/var/named/named.rev 文件的内容:

```

$TTL 86400
@      IN  SOA      s1. xyz.com.cn. root. xyz.com.cn. (
                                2001110600 ; serial
                                28800 ; refresh
                                14400 ; retry

```

```

        3600000 ; expire
        86400 ; minimum
    )
    IN NS xyz.com.cn.
201    IN PTR s1.xyz.com.cn.
202    IN PTR s2.xyz.com.cn.

```

【问题 1】该服务器是一个什么类型的域名服务器？

【问题 2】该服务器的域名守护程序利用什么文件去初始化高速缓存？

【问题 3】该域中电子邮件服务器的 IP 地址是什么？

【问题 4】(1)处应当填写什么内容？

【问题 5】/var/named/named.hosts 文件中阴影一行的作用是什么？

【问题 6】如果对上述文件进行了修改，如何使它立即生效？其命令是什么？(不重新启动计算机)

10. 阅读以下说明，回答问题 1~5，将解答填入对应的答案栏内。

【说明】

某公司使用了一台安装有 Linux 操作系统的 PC 服务器作为电子邮件服务器，邮件发送服务使用的为 sendmail 8.0，下面是 sendmail 的几个配置文件的片断：

/etc/sendmail.cf 文件片断：

```

Cwlocalhost
Fw/etc/mail/local-host-names

```

/etc/mail/access 文件内容：

```

localhost.localdomain    RELAY
localhost                RELAY
127.0.0.1                 RELAY
210.45.45                 RELAY
aapla.edu.cn              RELAY
_____ (1)

```

/etc/aliases 文件内容：

```

bin:          root
daemon:       root
adm:          root
lp:           root
sync:         root
shutdown:     root
halt:         root
mail:         root
webmaster:    zhang
net_center:   zhang, taoan, liwenglong
owner-net_group: zhang

```

【问题 1】在/etc/sendmail.cf 文件中并没指定该电子邮件服务器的主机名，但它却能接

收所有 abc.com.cn 域内的电子邮件，这个信息可能存放在哪儿？

【问题 2】该公司的员工最有可能在哪个网络中收发电子邮件？

【问题 3】在使用过程中，发现域 xyz.com.tw 上有人使用该服务器发送电子邮件，为了拒绝其访问，在(1)处该填写什么内容？

【问题 4】该公司主页上有一个电子邮件链接，邮件地址是 webmaster@abc.com.cn，单击它通过 Outlook Express 发送了一封电子邮件，该邮件将发送给谁？

【问题 5】命令 #/usr/bin/makemap /etc/mail/access.db</etc/mail/access 的作用是什么？

11. 阅读以下说明，回答问题 1~5，将解答填入对应的答案栏内。

【说明】

在 Linux 下安装配置 Wu-FTP 服务，FTP 服务程序需要读取配置一些文件，下面是几个 FTP 配置文件的主要内容：

/etc/ftpuser 文件的内容是：

```
root
uucp
news
bin
adm
nobody
lp
sync
shutdown
halt
mail
wang
```

/etc/ftphosts 文件的内容是：

```
allow * *.abc.com.cn 210.45.12.0/16 210.45.13.0/16
deny * *.hanker.com 131.222.154.0/24
```

/etc/ftpaccess 文件的内容是：

```
loginfails 5
class local real *
class remote anonymous guest *
limit remote 100 anonymous /etc/ftpd/toomany.msg
message /etc/ftpd/welcome.msg login
compress yes local remote
tar yes local remote
private yes
passwd-check none
log commands real
log transfer anonymous guest inbound outbound
log transfer real inbound
shutdown /etc/ftpd/shut.msg
```

```

delete no anonymous,guest
overwrite no anonymous,guest
rename no anonymous
chmod no anonymous,guest
umask no anonymous
upload /home/ftpd * no
upload /home/ftpd /bin no
upload /home/ftpd /etc no
upload /home/ftpd /pub yes real 0644 dirs
upload /home/ftpd /incoming yes real guest anonymous 0644 dirs
alias in /incoming
email admin@abc.net.cn
email ferd@sina.com.cn
deny *.com.tw /etc/ftpd/deny.msg

```

【问题 1】文件 `etc/ftpuser` 中包含了“wang”一行，其作用是什么？

【问题 2】从 FTP 客户端登录到该 FTP 服务器时，将显示什么内容？

【问题 3】该 FTP 服务器最多允许多少匿名用户同时登录？超过这个限制时 FTP 服务器如何响应客户机？

【问题 4】匿名用户登录时需要用什么密码验证？

【问题 5】文件 `/etc/ftpaccess` 中阴影部分语句的作用是什么？

12. 阅读以下说明，回答问题 1~5，将解答填入对应的答案栏内。

【说明】

图 3.127 是某一小型公司网络拓扑图，其中代理服务器的两块网卡的设置已在图中标出。

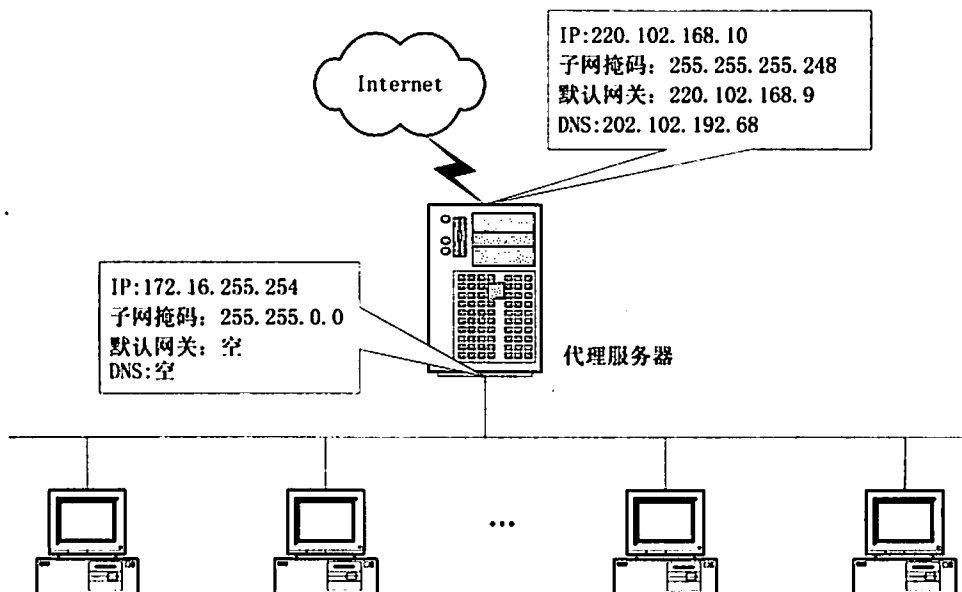


图 3.127 练习 12 拓扑图



该代理服务器使用基于 Linux 的 Squid 代理服务器，下面该服务器中文件 `/etc/squid/squid.conf` 的内容片断。

```
http_port 8080
cache_mem 256 MB
cache_dir /cache1 4000 24 33
cache_access_log /usr/local/squid/logs/access.log
cache_log /usr/local/squid/logs/cache.log
dns_nameservers _____ (1)
acl denydomain dstdomain foo.com.tw
acl all scr 0.0.0.0/0.0.0.0
http_access deny denydomain
http_access allow all
cache_mgr administrator@abc.com.cn
```

【问题 1】该公司的主机的 IP 地址范围是什么？子网掩码是什么？

【问题 2】客户机的 IE 的代理服务器端口号应设置为多少？(采用传统代理)

【问题 3】该代理服务器缓冲区放在哪里？大小是多少？能建多少一级目录，多少二级目录？

【问题 4】(1)处该填入什么内容？

【问题 5】文件中阴影部分两行语句的作用是什么？

13. 某单位的网络要配置一台 DHCP 服务器，为网络内部的计算机自动分配 IP 地址。在考虑 DHCP 服务器时，回答以下问题。

【问题 1】客户机启动时是如何从 DHCP 服务器得到动态 IP 的？

【问题 2】DHCP 客户机在启动时并没有 IP 地址，也不知道 DHCP 服务器地址，那么它与 DHCP 服务器之间是通过什么方式进行通信的？

【问题 3】配置 DHCP 服务器应具备什么条件？

【问题 4】Windows 2000 用户通过什么命令可以看到自己租约到的本机 IP 地址？用何命令可以重新向 DHCP 服务器租约 IP？用何命令可以释放 IP？

14. 阅读以下说明，回答问题 1~5，将解答填入对应的答案栏内。

【说明】

在 Linux 下安装配置 Apache 服务，Apache 服务程序 `httpd` 启动时需要读取配置文件 `httpd.conf`，以下是一个 `httpd.conf` 配置文件的片断：

```
## httpd.conf -- Apache HTTP server configuration file
### Section 1: Global Environment
ServerType standalone
ServerRoot "/etc/httpd"
Timeout 300
KeepAlive On
MaxKeepAliveRequests 100
KeepAliveTimeout 15
MaxClients 150
### Section 2: 'Main' server configuration
```

```
Port 80
User apache
Group apache
ServerAdmin webmaster@abc.com.cn
ServerName www.abc.com.cn
DocumentRoot "/var/www/html"
UserDir public_html
DirectoryIndex index.html
Alias /jianji "/home/zhang/jianji"
ScriptAlias /cgi-bin/ "/var/www/cgi-bin/"
ErrorDocument 404 /missing.html
### Section 3: Virtual Hosts
NameVirtualHost 192.168.10.101
<VirtualHost 192.168.10.101>
    ServerAdmin webmaster@abc.com.cn
    DocumentRoot /www/htdocs/abc
    ServerName markert.abc.com.cn
    ErrorLog logs/host.some_domain.com-error_log
    CustomLog logs/host.some_domain.com-access_log common
</VirtualHost>
```

【问题 1】该 Web 服务器的工作目录是什么？

【问题 2】当用户在要访问该 Web 服务器的一个文件，但这个文件已经被删除了，服务器如何响应客户？

【问题 3】httpd.conf 文件中阴影部分语句的作用是什么？

【问题 4】当用户在浏览器中输入 http://192.168.10.100/~zhang/时，将访问什么内容？

【问题 5】停止 Apache 服务器的命令是什么？

### 3.9.2 参考答案

1.

【问题 1】B 类地址、190.190.0.0、190.190.255.255

【问题 2】255.255.0.0

【问题 3】190.190.144.0、190.190.159.255、190.190.144.1~190.190.159.254

2.

【问题 1】255.255.255.224

【问题 2】30

【问题 3】196.102.56.192

【问题 4】196.102.56.223

3.

【问题 1】255.255.255.248

【问题 2】222.34.109.64

【问题 3】222.34.109.71

4. 【问题1】255.255.255.224、255.255.255.248和255.255.255.252：下图3.128是一种划分方法：

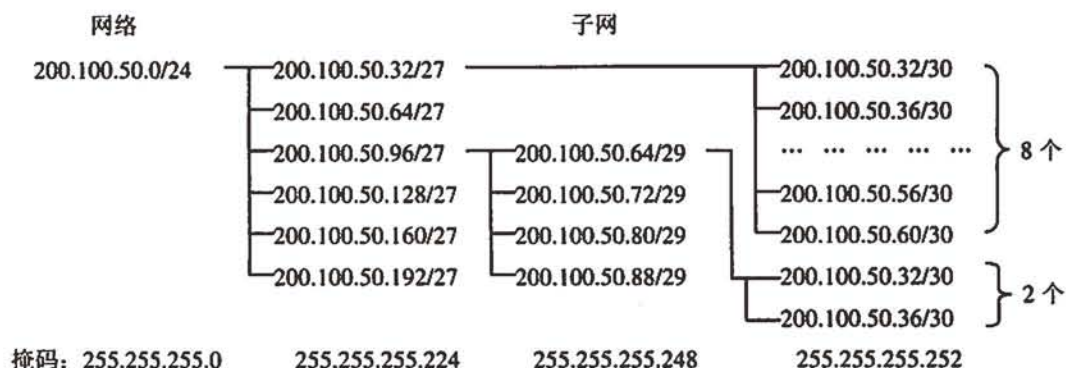


图 3.128 问题1 解答

【问题2】略

【问题3】略

5. (1)C      (2)B      (3)B      (4)A      (5)A

6. (1)B      (2)C      (3)A      (4)A      (5)C

7. (1)D      (2)B      (3)C      (4)D      (5)A

8. (1)A      (2)D      (3)B      (4)C      (5)A

9.

【问题1】主域名服务器

【问题2】/var/named/named.ca

【问题3】199.168.10.201

【问题4】10.168.199.in-addr.arpa

【问题5】定义一个主机别名

【问题6】重新启动 DNS 服务，其命令是#/etc/rc.d/init.d/named restart

10.

【问题1】存放在/etc/mail/local-host-names 文件中

【问题2】210.45.45.0/24 这个 C 类网络中

【问题3】xyz.com.tw      DENY

【问题4】将发给 zhang 这个用户，邮件服务器地址是 zhang@abc.com.cn

【问题5】创建传送控制配置文件 access 相应的数据库文件

11.

【问题1】禁止用户 wang 使用 FTP 登录

【问题2】将显示文件/etc/ftpd/welcome.msg 中内容

【问题3】100、用/etc/ftpd/toomany.msg 文件中内容响应客户

【问题4】任意密码

【问题5】拒绝域 com.tw 内的用户 FTP 登录，该域若有用户登录将用/etc/ftpd/deny .msg 文件内容响应客户

12.

【问题 1】172.16.0.1 至 172.168.255.253、255.255.0.0

【问题 2】8080

【问题 3】/cache1、4000M、24、33

【问题 4】202.102.192.68

【问题 5】禁止客户访问域 foo.com.tw 内的所有主机

13.

【问题 1】请求 IP 租约、提供 IP 租约、选择 IP 租约和确认 IP 租约

【问题 2】广播方式

【问题 3】DHCP 服务器应具有静态 IP 和子网掩码，有一组可供分配的 IP 地址

【问题 4】ipconfig/all、ipconfig/renew、ipconfig/release

14.

【问题 1】/etc/httpd

【问题 2】将文档/missing.html 来回应客户浏览器

【问题 3】建立一个域名为 markert.abc.com.cn 的虚拟 Web 服务器(虚拟主机)，并指定相应的参数

【问题 4】访问该服务器中用户 zhang 的主目录下 public\_html 子目录的索引文件 index.html，若该文件不存在就会出错

【问题 5】#/etc/init.d/httpd stop



## 第4章 Web 网站建设

大纲要求:

- 掌握 Web 网站的建立、管理与维护方法,熟悉网页制作技术。
- Web 网站基础,主要包括 Web 网站的规划、建立、管理与维护。
- 动态网页技术,主要包括 JSP、ASP、XML 等动态网页编程技术的基本概念和动态网页创作。
- 网页制作工具,主要包括使用 HTML 和相关软件进行网页设计与制作(如选用 Photoshop、Flash、Fireworks 或 Dreamweaver 等)。

### 4.1 使用 HTML 制作网页

#### 4.1.1 考点辅导

##### 4.1.1.1 HTML 简介

HTML(Hyper Text Mark-up Language, 超文本标记语言)是 WWW 的描述语言。它是标准通用型标记语言(SGML, Standard Generalized Markup Language)的一个应用。

##### 1. HTML 元素

HTML 是标准的 ASCII 文档。其扩展名通常是.html、.htm、.mht、.mhtml 或.shtml, 这是常见的 5 种格式。从结构上讲, HTML 由元素组成, 它用成对的标签(tag), 即起始标签和结束标签来组织和定义文档的显示格式。HTML 文件中 HTML 标签的语法格式如下:

<标签名称>标签对象</标签名称>

##### 2. HTML 文档的组成

HTML 文档以<html>标签开始, 以</html>标签结束, 由文档头和文档体两部分构成。文档头以<head>标签开始, 以</head>标签结束; 文档体以<body>标签开始, 以</body>标签结束。

文档头部分可以包含以下元素:

- (1) 窗口标题。HTML 文档的简单描述, 对应标签为<title></title>。
- (2) 脚本语言。浏览器解释执行的语句, 对应标签为<script></script>。
- (3) 样式定义。样式表主要用于格式化网页中的元素, 对应标签为<style></style>。
- (4) 元数据。主要提供超本文档内容和主题的信息, 对应标签为<meta>。

文档体包含了可以在浏览器中显示的内容, 包含以下元素:

- (1) 文本。文本通常以格式化的内容放在文档体中。
- (2) 图像。图像主要用于丰富网页的内容。

(3) 链接。链接通常放在文档体中, 允许在网站中导航到其他网站。

(4) 多媒体和特定的编程事件。主要是指包含在 HTML 文档中的 Shockwave、Java Applet 或在线视频等。

### 3. HTML 文档的结构

HTML 文档的基本结构如下:

```
<html>
<head>
<title> </title>
...
</head>
<body>
...
</body>
</html>
```

#### 4.1.1.2 HTML 常用元素

##### 1. 基本元素

###### (1) 窗口标题(Title)

Title 是 HTML 文档的标题, 是对文档内容的概括, 在浏览 Web 页面时, 它会出现在浏览器的标题栏处。其使用格式为:

```
<title>窗口标题描述</title>
```

###### (2) 页面标题

页面标题有 6 种, 分别为 h1、h2、h3、h4、h5 和 h6, 用于表示页面中的各种标题。其使用格式为:

```
<hn>页面标题描述</hn> (n=1, 2, ..., 6)
```

标题具有对齐属性 align, 其属性值有 left(标题居左)、center(标题居中)和 right(标题居右)等。例如:

```
<h2 align="center">居中的二级页面标题</h2>
```

###### (3) 字体

HTML 的字体包括字体大小、字体风格、字体颜色和闪烁等。

- 字体大小: HTML 有 7 种字号, 1 号最小, 7 号最大, 默认字号为 3, 可以用<basefont size=字号>设置默认字号。
- 字体风格: 字体风格主要包括以黑体<b>、斜体<i>和下划线<u>为代表的物理风格以及特别强调<strong>、源代码<code>和示例<samp>等为代表的逻辑风格。
- 字体颜色: 字体颜色用<font color=#>指定, #可以是 6 位的十六进制数, 也可以是 black、navy 和 purple 等英文颜色名称。
- 闪烁: 标签<blink>文本</blink>使文本闪烁, 闪烁频率为一秒一次。

#### (4) 横线

横线，也称水平线，一般用于分隔文本。其 HTML 标签为：<hr>。可以指定水平线的对齐、颜色、阴影和高度等相关属性。如：

```
<hr align="center" color=blue noshade size="1">
```

表示设定水平线的格式为：居中对齐，蓝色，无阴影，高度为 1。

#### (5) 分行和禁止分行

HTML 标签<br>，表示在此处分行。<nobr>...</nobr>表示通知浏览器：其中的内容在一行内显示，若一行显示不了，则超出部分被裁减掉。

#### (6) 分段

HTML 的分段完全依赖于分段标签<p>段落文本</p>。<p>也可以设定对齐、风格等。如：

```
<p align="left" style="color:#FF0000 ">
```

表示该段落格式为：左对齐、字体颜色为红色。

#### (7) 转义字符

HTML 使用的字符集是 ISO &859 Latin-1 字符集，该字符集中有许多在标准键盘上无法输入的字符。对于这些字符只能使用转义字符。常见的需要转义的字符有<、>、&和引号等。

<的转义序列为&lt;或&#60;，>的转义序列为&gt;或&#62;，引号的转义序列为&quot;或&#34;。例如：

```

```

注意：

转义序列各字符间不能有空格，转义字符必须以“;”结束，单独的&不被认为是转义的开始。

#### (8) 背景和文本颜色

窗口背景和文本可以使用以下标签指定：

```
<body background="image-URL"></body>
```

```
<body bgcolor="# " text="# " link="# " alink="# " vlink="# "></body>
```

background 表示背景图片；image-URL 代表背景图片的 URL 地址；bgcolor 指背景颜色，其中#后面是指定的十六进制的红、绿、蓝分量；text 表示文本颜色；link 表示链接颜色；alink 表示活动链接颜色；vlink 表示已访问过的链接颜色。

例如：

```
<body background="images/bg.gif" bgcolor="#FFFFFF" text="#000000"
link="#FF0000" alink="#0000FF" vlink="#FF00FF" ></body>
```

这表示页面背景图片是 images 文件夹下的 bg.gif 文件，页面背景颜色为白色，文本颜色为黑色，链接颜色为红色，活动链接为蓝色和已访问过链接为粉红色。

### (9) 图像(Image)

图像主要用于网页美工。

其使用的基本格式为:

```

```

其中, image-URL 是图像文件的 URL, width 和 height 表示图像文件的宽度和高度。

另外可选的图像属性还包括 alt、align 以及 vspace 和 hspace 等, 其中 alt 是指图像的替代文字, align 指图像的对齐属性, vspace 和 hspace 表示文本与图像的纵向和横向间距。

例如:

```

```

### (10) 列表(List)

列表主要用于列举条目, 常用的列表有 3 种格式, 即无序列表、有序列表和自定义列表。

无序列表: 以<ul>开始, 每一列表条目用<li>引导, 编号用黑点表示, 最后是</ul>。  
例如:

```
<ul>  
<li>昨天</li>  
<li>今天</li>  
<li>明天</li>  
</ul>
```

有序列表: 以<ol>开始, 每一列表条目用<li>引导, 编号用数字表示, 最后是</ol>。  
例如:

```
<ol>  
<li>昨天</li>  
<li>今天</li>  
<li>明天</li>  
</ol>
```

自定义列表: 以<dl>开始, 每一列表条目用<dt>引导, 编号用<dd>标签的内容表示, 最后是</dl>。例如:

```
<dl>  
<dt>昨天</dt>  
<dd>yesterday</dd>  
<dt>今天</dt>  
<dd>today</dd>  
</dl>
```

## 2. 超文本链接

超文本链接一般由两部分组成: 一是被指向的目标, 二是指向目标的链接。

### (1) 统一资源定位器(URL)



用于指定访问文档的方法。一个 URL 的标准构成为:

Protocol://machine.name[:port]/directory/filename

其中, Protocol 是指访问该资源所采用的协议,它可以是 http(超文本传输控制协议)、ftp(文件传输控制协议)或 news(网络新闻资源)等; machine.name 是指存放资源的主机 IP 或域名; port 是指用于存放资源的主机的相关服务的端口号; directory 和 filename 是该资源的路径和文件名。

例如:

`http://www.microsoft.com`

## (2) 超级链接标签

在 HTML 文档中用链接指向一个目标,其基本格式为:

`<a href="URL">字符串</a>`

例如:

`<a href="http://www.yahoo.com">雅虎搜索</a>`

## (3) 标记

标记,也可称为书签或锚记。标识一个链接目标的方法为:

`<a href="name">text</a>`

其中, name 为放置 HTML 文档的全文惟一的标记串,可以用下列方法来指向它:

`<a href="URL#name">text</a>`

例如:

`<a href="http://www.sina.com.cn/sports/news.htm# import">欧洲赛事</a>`

## (4) 图像链接

图像也可以建立超级链接,其格式为:

`<a href="URL"> </a>`

例如:

`<a href="http://www.macromedia.com"></a>`

## (5) 图像地图

图像地图可以把图像分成多个区域,每一区域指向不同的目标。图像地图可以分为服务器端和客户端地图。服务器端图像地图的使用格式为:

`<a href="/cgi-bin/imagemap/mymap.map">`

`</a>`

其中, mymap.map 是存放在服务器端/cgi-bin/imagemap 目录下的图像地图的分区信息文件。客户端图像地图的使用格式为:

```

```

其中, image-URL 为用作图像地图的图像, usemap 指客户端地图的标记名。

客户端图像地图的分区信息用<map name="mapname">说明。图像地图的各个区域用<area shape="形状" coords="坐标" href="URL">说明。形状可以是矩形、圆形或多边形。

例如:

```

<map name="Map">
  <area shape="rect" coords="74,100,150,184" href="first.htm">
  <area shape="circle" coords="314,230,65" href="second.htm ">
  <area shape="poly" coords="39,357,166,369,183,313,129,263,49,304"
href="third.htm">
</map>
```

### 3. 表格(Table)

表格通常用于组织和排列网页信息。表格由<table >开始, 以</table >结束, 表格的内容由<thead>、<tbody>、<th>、<tr>和<td>定义。

其基本格式如下:

```
<table>
  <thead>
    <tr>
      <th>... </th>
    ...
  </tr>
</thead>
<tbody>
  <tr>
    <td>...</td>
  ...
</tr>
...
</tbody>
</table>
```

其中, <thead>是表头标签, <tbody>是表格的主体, <th>是列标题标签, <tr>是行标签, <td>是列标签。

例如:

```
<table width="200" border="1" bgcolor="#CCCCCC">
<thead>
  <tr>
    <th scope="col">姓名</th>
    <th scope="col">性别</th>
    <th scope="col">爱好</th>
  </tr>
```

```
</thead>
<tbody>
  <tr>
    <td>李湘湘</td>
    <td>女</td>
    <td>电视主持</td>
  </tr>
  <tr>
    <td>冯孝余</td>
    <td>男</td>
    <td>电子音乐</td>
  </tr>
</tbody>
</table>
```

#### 4. 框架(Frame)

框架的作用是将浏览器窗口分成多个区域，每个区域可以单独显示一个 HTML 文档，各个区域的文档可以有关联地显示相关内容。

框架的基本结构如下：

```
<html>
<head>
<meta http-equiv="Content-Type" content="text/html; charset=gb2312">
<title>... </title>
</head>
<frameset>
  <frame src="URL" name="leftFrame">
  <frame src="URL" name="mainFrame">
  ...
</frameset>
<noframes>
<body>
</body>
</noframes>
</html>
```

框架中可以放置相应的 HTML 页面，主要通过以下标签来完成。

##### (1) <frameset> 标签

框架集标签，基本参数包括 frameborder、border 和 framespacing 等，主要用于定义整个框架集的行列及边界参数。

##### (2) <frame> 标签

单独框架标签，基本参数包括 src 和 name 等，主要是指定填充该框架的 HTML 文档属性。

##### (3) <noframe> 标签

当浏览器不支持框架时，就显示该标签中的内容。

例如:

```
<html>
<head>
<meta http-equiv="Content-Type" content="text/html; charset=gb2312">
<title>上方固定左侧嵌套</title>
</head>
<frameset rows="80,*" cols="*" frameborder="NO" border="0"
framespacing="0">
  <frame src="top.htm" name="topFrame" scrolling="NO" noresize >
  <frameset cols="80,*" frameborder="NO" border="0" framespacing="0">
    <frame src="left...htm" name="leftFrame" scrolling="NO" noresize>
    <frame src="main.htm" name="mainFrame">
  </frameset>
</frameset>
<noframes>
<body>
</body>
</noframes>
</html>
```

## 5. 表单(Form)

表单是网页中一种重要的信息收集和交流工具,它在 Web 数据库技术中起到关键性的作用。一个包含简单表单对象的 HTML 文本如下所示:

```
<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01 Transitional//EN"
"http://www.w3.org/TR/html4/loose.dtd">
<html>
<head>
<meta http-equiv="Content-Type" content="text/html; charset=gb2312">
<title>百度搜索</title>
</head>
<body>
<FORM name=f action=http://www.baidu.com/baidu method="post"><INPUT
class=ff
  maxLength=100 size=35 name=w>
  <INPUT type=submit value=百度搜索>
</FORM> </FORM>
</body>
</html>
```

### (1) 表单标签

标签<FORM>提供表单的功能,由开始和结束标签<FORM>和</FORM>组成,表单中可以设置文本框、按钮或下拉菜单等表单域元素。在开始标签中带有两个重要属性:action 和 method,分别指定了表单的动作和方法。



### (2) 文本框

文本框可以分为单行文本框和多行文本框。单行文本框的 HTML 基本标签是: `<input type="text" name="textfield">`; 多行文本框的 HTML 基本标签是: `<textarea name="textfield"></textarea>`。

### (3) 按钮

按钮可以分为单选按钮、多选按钮以及提交和重置按钮。单选按钮的 HTML 基本标签是: `<input type="radio" name="radiobutton" value="radiobutton">`; 多选按钮的 HTML 基本标签是: `<input type="checkbox" name="checkbox" value="checkbox">`; 提交和重置按钮的 HTML 基本标签分别是: `<input type="submit" name="Submit" value="提交">`和`<input type="reset" name="Submit" value="重置">`。

### (4) 下拉菜单

下拉菜单通过标签`<select>`实现, 其 HTML 基本标签是: `<select name="select" size="1"></select>`。

#### 4.1.1.3 HTML 应用实例

以下是著名的 Google 搜索引擎首页的 HTML 源文件(注: 为了方便读者阅读, 笔者进行了重新排版):

```
<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.0 Transitional//EN">
<HTML><HEAD><TITLE>Google</TITLE>
<META http-equiv=content-type content="text/html; charset=UTF-8">
<STYLE>
  BODY {FONT-FAMILY: arial,sans-serif}
  TD {FONT-FAMILY: arial,sans-serif }
  A {FONT-FAMILY: arial,sans-serif }
  P {FONT-FAMILY: arial,sans-serif }
  .h {FONT-FAMILY: arial,sans-serif}
  .h {FONT-SIZE: 20px}
  .q {COLOR: #0000cc}
</STYLE>
<SCRIPT>
<!--
  function sf(){document.f.q.focus();}
  function clk(el,ct,cd,sg)
  { if(document.images)
    { (new Image()).src="/url?sa=T&ct="+escape(ct)+
      "&cd="+escape(cd)+"&url="+escape(el.href).replace(/\+/g,"%2B")+
      "&ei=WXG6Qs3eO6qmOMPehZwP"+sg;}
    return true;}
  function rbi(f)
  { if (navigator.appName == "Netscape")
    { f.biw.value=self.innerWidth;}
    else { f.biw.value=document.body.clientWidth;}}// -->
</SCRIPT>
```



```

</FONT></TD></TR>
<TR>
  <TD align=middle colSpan=3><FONT size=-1>
    <INPUT id=all type=radio CHECKED value="" name=lr>
    <LABEL for=all>搜索所有网页</LABEL>
    <INPUT id=ch type=radio value=lang_zh-CN|lang_zh-TW name=lr>
    <LABEL for=ch>搜索所有中文网页</LABEL>
    <INPUT id=il type=radio value=lang_zh-CN name=lr>
    <LABEL for=il>搜索简体中文网页</LABEL>
  </FONT></TD></TR></TBODY></TABLE></FORM>
<p><FONT size=-1><p></FONT> <BR>
<p><BR><BR><FONT size=-1>
<A href="http://www.google.com/intl/zh-CN/ads/">广告计划</A> -
<A href="http://www.google.com/intl/zh-CN/about.html">Google 大全</A> -
<A href="http://www.google.com/ncr">Google.com in English</A>
<SPAN id=hp style="BEHAVIOR: url(#default#homepage)"></SPAN>
<SCRIPT>
//<!--
  if (!hp.isHomePage('http://www.google.com/'))
  { document.write("<p><a href=\""/mgyp.html\"
    onClick=\"style.behavior='url(#default#homepage)';
    setHomePage('http://www.google.com/');\">将 Google 设为首页! </a>");)
//-->
</SCRIPT>
</FONT>
<P><FONT size=-1>©2005 Google - 搜索 8,058,044,651 张网页</FONT></P>
</CENTER></BODY></HTML>

```

该文档在 IE 浏览器中的运行结果如图 4.1 所示。

相关 HTML 代码说明：

- (1) <TITLE>Google</TITLE>, <TITLE>定义网页的标题是 Google。
- (2) <STYLE>BODY {FONT-FAMILY: arial,sans-serif}...</STYLE>, <STYLE>定义了网页元素的样式。
- (3) <SCRIPT><!--function sf(){...}...// --></SCRIPT>, <SCRIPT>定义了网页使用的 Java Script 的函数。
- (4) <IMG height=110 alt=Google src="Google.files/logo.gif" width=286>, <IMG>定义了网页中所使用的 LOGO 图片。
- (5) <TABLE cellSpacing=0 cellPadding=4 border=0>...</TABLE>, <TABLE>定义了以表格方式排列的网页数据。
- (6) <FORM name=f action=/search>...</FORM>, <FORM>定义了网页中的一个表单对象。
- (7) <INPUT type=hidden value=zh-CN name=hl>, <INPUT>定义了一个隐含域类型的网页输入数据。
- (8) <LABEL for=ch>搜索所有中文网页</LABEL>, <LABEL>定义了表单中的标签

对象。

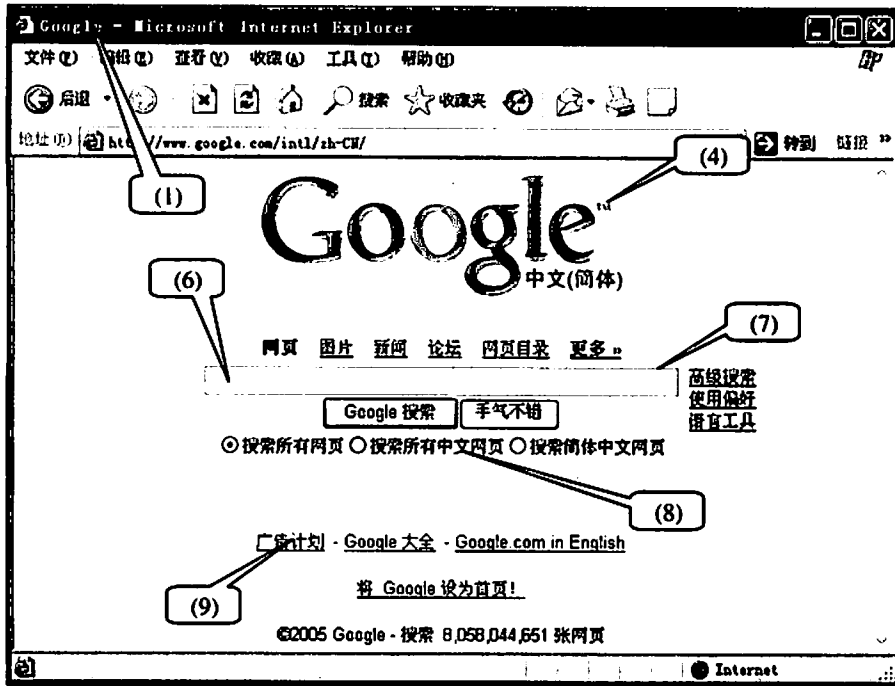


图 4.1 Google 首页

(9) `<A href="http://www.google.com/intl/zh-CN/ads/">广告计划</A>`, `<A>`定义了网页中的一个超级链接地址。

#### 4.1.2 典型例题分析

例 1 阅读下列 HTML 文本和说明,在该 HTML 文本中存在 5 处错误,请指出错误所在的行号、错误原因以及改正的方法,把解答填入答案的对应栏内。(2001 年网络程序员级下午试题二)

##### 【说明】

这是一个简单的 HTML 文本,显示作者个人主页的登录界面。

##### 【HTML 文本】

- (1) `<HTML>`
- (2) `<BODY>`
- (3) `<HEAD>`
- (4) `<META NAME="Author" CONTENT="Brent Heslop, David Holzgang">`
- (5) `</HEAD>`
- (6) `<TITLE TITLE="Authors Home Page">`
- (7) `<!-- MAKE SURE BKGND COLOR IS WHITE -->`
- (8) `<BGCOLOR="white">`
- (9) `<IMG ALT="log.jpg" SRC="Welcome to Authors Home page">`
- (10) `<H2><A HREF="http://WWW.authors.public.com">Authors Home Page</A><H2>`



- (11) <P>Welcome to the authors Web Site. </P>
- (12) </BODY>
- (13) <HTML>

分析：本题主要考核 HTML 语言的基本概念和元素。

HTML 文档以<HTML>标签开始，以</HTML>标签结束，由文档头和文档体两部分构成。文档头由<HEAD>开始，</HEAD>结束；文档体由<BODY>开始，</BODY>结束。

HTML 元素主要包括基本标签、列表、超级链接、图像、图像映射、表格、多媒体、表单和框架等。本题仅仅涉及了部分基本标签和图像等元素。

答案：

(1) 第(2)行不正确：<BODY>标签的位置不正确。<BODY>和</BODY>作为文档体标签，应该置于<HEAD>和</HEAD>之后。

(2) 第(6)行不正确：<TITLE>标签的使用不正确。<TITLE>和</TITLE>用于定义网页的标题，两个标签之间为标题的内容；并且<TITLE>和</TITLE>标签应位于<HEAD>和</HEAD>标签之间。

(3) 第(8)行不正确：<BGCOLOR="white">使用不正确。网页背景是通过<BODY>标签的 BGCOLOR 属性指定，如<BODY BGCOLOR="white">。

(4) 第(9)行不正确：<IMG ALT="log.jpg" SRC="Welcome to Authors Home page">使用不正确。<IMG>标签的 ALT 属性是指替代文本，SRC 属性是指图片源文件，因此 ALT 属性值和 SRC 属性值应该对调。

(5) 第(10)行不正确：<H2> 二级标题标签和<A>超级链接标签的顺序不正确，应该调整为：<A HREF="http://WWW.authors.public.com"><H2>Authors Home Page <H2></A>

例2 阅读下列说明和 HTML 文本。在 HTML 文本中存在 5 处错误，请指出错误之处并给出改正的方法。(2002 年网络程序员级下午试题三)

### 【说明】

这是一个简单的 HTML 文本，描述了框架的 HTML 语法，显示效果如图 4.2 所示。

### 【HTML 文本】

- (1) <html>
- (2) <head>
- (3) <title>框架测试</title>
- (4) </head>
- (5) <meta name="GENERATOR" content="Microsoft FrontPage 4.0">
- (6) <frameset rows="64, \*">
- (7) <frame name="banner" scrolling="no" target="contents" src="header.htm">
- (8) <frame name="contents" target="list" src="list.htm">
- (9) <frameset cols="150, \*">
- (10) <frame name="main" src="context.htm">
- (11) </frameset>
- (12) </frameset>
- (13) <noframes>
- (14) <body><p>此网页使用了框架。</body>

(15)</noframes>

(16)</html>

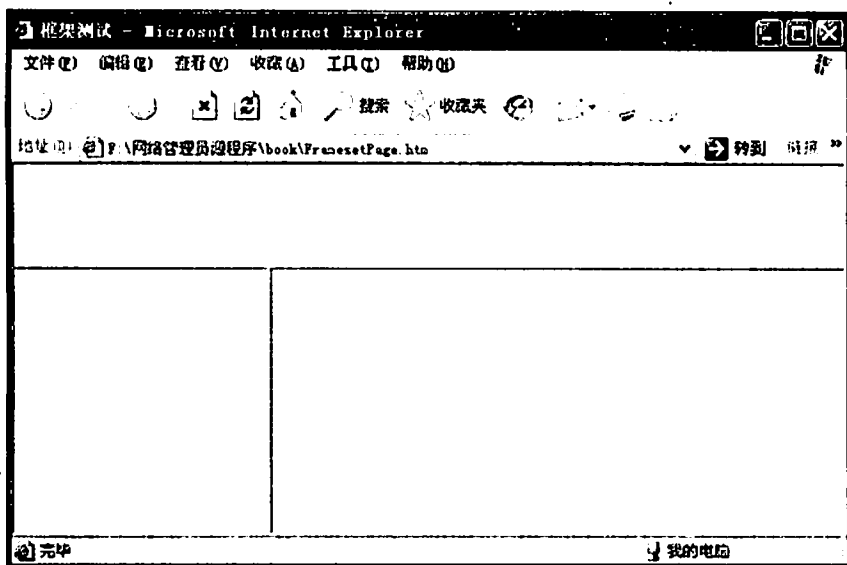


图 4.2 HTML 框架效果

分析：本题主要考查考生对 HTML 文档和框架网页结构的掌握情况。<frameset>标签是一个框架容器，它可以将窗口分成若干个框架，框架的 HTML 标签是<frame>。<frame>的个数是由<frameset>标签中的参数决定的。<frameset>标签中还可能包含一个可选的<noframes>标签，其作用是，当浏览器不支持或禁用<frame>时，<noframes>标签将提供替代的浏览内容。

答案：

(1) 第(5)行位置不正确：<meta>标签必须位于<head>与</head>标签之间。

(2) 第(8)行不正确：在<frame>的 target 属性中指定的框架“list”在文本中没有定义，可以改为 banner、contents 或 main 三个中的任何一个。

(3) 第(9)行位置不正确：根据图像分析，框架结构应该为上左右型，而本例为左右下型，应将第(8)、(9)行互调。

(4) 第(13)、(14)、(15)行位置不正确：<noframes>与</noframes>应位于<frameset>与</frameset>之间。

(5) 第(14)行不正确：<p>与</p>应该成对出现，在文字与</body>之间应添加</p>。

例 3 请根据网页显示的效果图和网页中的元素说明，将 HTML 文本中 (n) 处的解答填入答案的对应栏中。(2003 年网络程序员级下午试题三)

【说明】

在 IE 浏览器中输入 yoyo 电子邮局主页地址并按回车键后，网页的显示效果如图 4.3 所示。

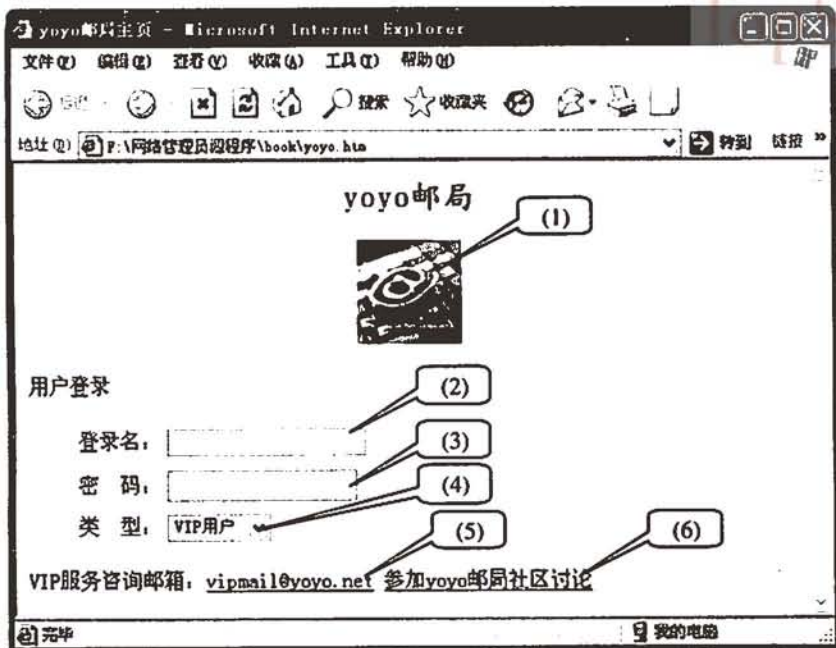


图 4.3 yoyo 电子邮局主页在 IE 中刚打开时的效果图

序号	类型	说明
(1)	图片	文件名: "atmail.jpg"; 宽度: 80pixels; 高度: 80pixels
(2)	【登录名:】文本框	名称: "login_name"; 尺寸: 20 字符
(3)	【密码:】密码文本框	名称: "login_password"; 尺寸: 20 字符
(4)	【类型:】下拉列表框	下拉列表项: "商务用户"、"VIP 用户"、"免费用户"
(5)	发送电子邮件超链接	邮件发送地址: "vipmail@yoyo.net"
(6)	BBS 超链接	超链接地址: "http://bbs.yoyo.com"

## 【HTML 文本】

```

<html>
<head>
<title>yoyo 邮局主页</title>
</head>
<body>
<p align="center">
<b><font color="#800080" face="楷体_GB2312" size="5">yoyo 邮局</font></b>
</p>
<p align="center">
(1)
</p>
<p align="left"> </p>
<p align="left">用户登录</p>
<table>
<tr><td width="100" height="16">

```

```

        <div align="right">
            登录名:
        </div></td>
            _____
                (2)
</table>
<table>
    <tr><td width="100" height="16">
        <div align="right">
            密 码:
        </div></td>
            _____
                (3)
    </td>
</table>
<table>
    <tr><td width="100">
        <div align="right">
            类 型:
        </div></td>
        <select onchange="changeBackURL()" name="select">
            <option>商务用户</option>
            _____
                (4)
            <option>免费用户</option>
        </select>
    </td>
</table>
    <p></p><p></p>
    VIP 服务咨询邮箱: _____ (5)
    <a href="http://bbs.yoyo.com">参加 yoyo 邮局社区讨论</a>
</body>
</html>

```

分析: 本题主要考查考生对 HTML 网页元素标签的掌握情况。

HTML 元素主要包括基本标签、列表、超级链接、图像、图像映射、表格、多媒体、表单和框架等。本题中主要涉及图片、单行文本框、下拉菜单和电子邮件的超级链接等。

答案:

- (1) 
- (2) <input name="login\_name" size="20">
- (3) <input type="password" name="login\_password" size="20">
- (4) <option selected>VIP 用户</option>
- (5) <a href="mailto:vipmail@yoyo.net">vipmail@yoyo.net</a>

例 4 请根据网页显示的效果图的网页中元素说明, 将 HTML 文本中 (n) 处的解答填入对应的答案栏内。(2004 年下半年网络管理员级下午试题五)

【说明】

在浏览器的地址栏中输入常春藤大学招生办公室主页的网址并按回车后键, 网页显示的效果如图 4.4 所示。



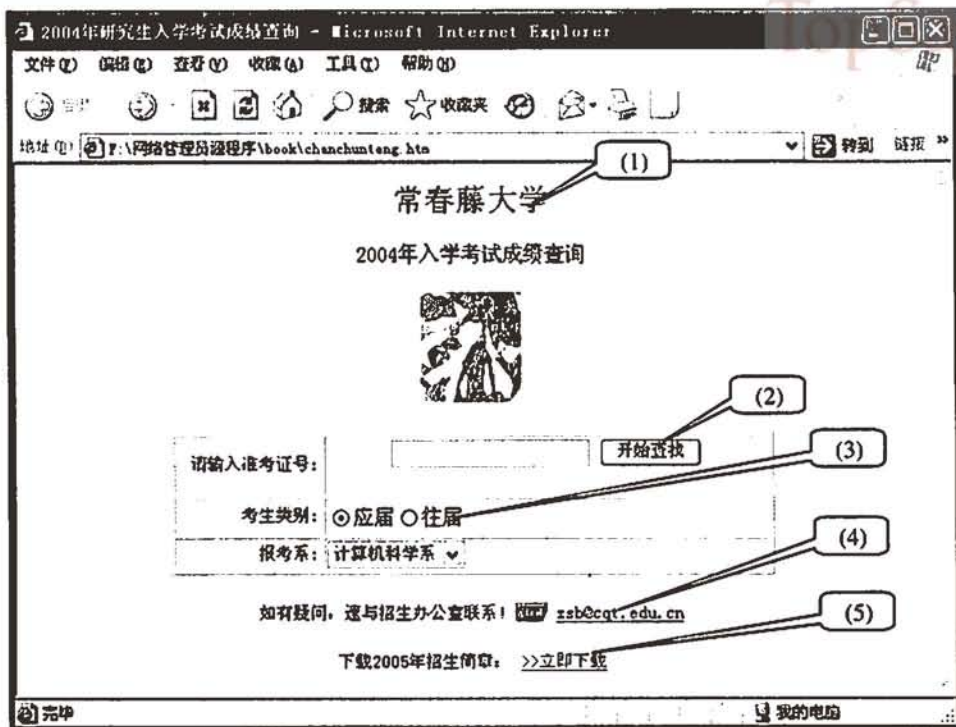


图 4.4 长春藤大学招生办公室主页

## 【HTML 文本】

```

<html>
<head>
<meta http-equiv="Content-Type" content="text/html; charset=gb2312">
<title>2004 年研究生入学考试成绩查询</title>
(1)

<body bgcolor="white">
(2)

<p align="center">2004 年入学考试成绩查询</p>
<p align="center">
</p>
<div align="center" style="width:679; height:101 ">
<table width="63%" height="17" border="1" >
  <tr>
    <td width="23%" height="1">
      <p align="right"><font face="宋体" size="2">请输入准考证号:</font></p>
    </td>
    <td width="46%" height="1">
      <p align="left">
        <input type="text" name="T1" size="20">
      </p>
    </td>
  </tr>
</table>
(3)

```

```

        <input type="submit" value="开始查找" name="B1"></p>
    </form>
    </td>
</tr>
<tr>
    <td width="23%" height="17">
        <p align="right"><font size="2">考生类别:</font></p>
    </td>
    <td width="38%" height="19" align="left">
        (4)
    </td>
</tr>
<tr>
    <td width="23%" height="1">
        <p align="right"><font size="2">报考系:</font></p>
    </td>
    <td width="46%" height="1">
        <p align="left"><select size="1" name="D1">
            <option selected>计算机科学系</option>
            <option>机械工程系</option>
            <option>中文系</option>
        </select>
    </p>
    </td>
</tr>
</table>
</div>
<p align="center"><font size="2">如有疑问, 速与招生办公室联系!
    (5)
<a href="mailto:vipmail@cqt.edu.cn">zsb@cqt.edu.cn</a></font>
</p>
<p align="center"><font size="2">下载 2005 年招生简章: </font>
    (6)
<font size="2" color="red"> &gt;&gt;立即下载</font></a></p>
</body>
</html>

```

分析: 本题主要考查考生对 HTML 网页元素标签的掌握情况。

HTML 元素主要包括基本标签(如字体)、列表、超级链接、图像、图像映射、表格、多媒体、表单和框架等。本题中主要涉及字体、表单、单选按钮、图像和文档下载的超级链接等基本元素。

答案:

- (1) </head>
- (2) <font color="blue" face="宋体" size="5">常春藤大学</font>
- (3) <form name="frmSearch" method="post" action="http://www.server.com/cgi-bin/program">

- (4) `<input name="type" type="radio" value="应届" checked>应届`  
`<input name="type" type="radio" value="往届">往届`  
 (5) ``  
 (6) `<a href="http://download.cqt.edu.cn/zsjz2005.doc">`

### 4.1.3 同步练习

1. 阅读下面 HTML 文本和说明, 在 HTML 文本中存在 5 处错误, 请指出这些错误并给出改正的方法。

#### 【说明】

这是一个简单的 HTML 文档, 显示的是一个网页列表信息, 显示界面如图 4.5 所示。

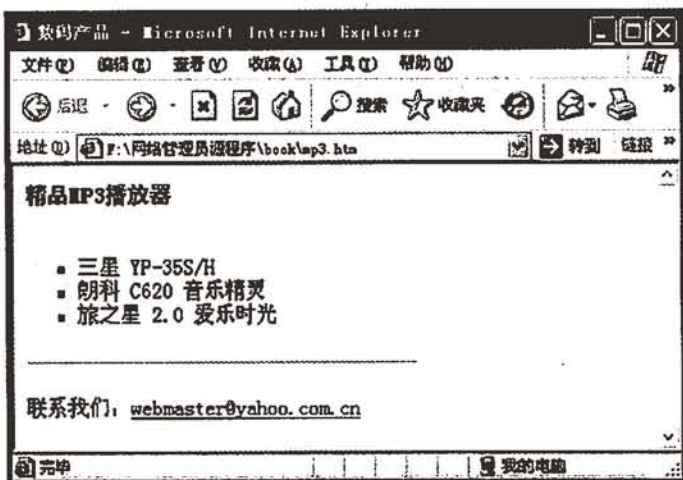


图 4.5 网页列表

#### 【HTML 文本】

- (1) `<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01 Transitional//EN"`
- (2) `"http://www.w3.org/TR/html4/loose.dtd">`
- (3) `<html>`
- (4) `<head>`
- (5) `<meta http-equiv="Content-Type" content="text/html; charset=gb2312">`
- (6) `</head>`
- (7) `<title>数码产品</title>`
- (8) `<body>`
- (9) `<p><strong>精品 MP3 播放器</p></strong>`
- (10) `<ul type="square">`
- (11) `<li>三星 YP-35S/H</li>`
- (12) `<li>朗科 C620 音乐精灵</li>`
- (13) `</ul>`
- (14) `<li>旅之星 2.0 爱乐时光</li>`

```
(15) <hr align="left" width="300" size="1">
(16) <p>联系我们:
(17) <a href="mailto:webmaster@yahoo.com"> </a> webmaster@yahoo.com.cn </p>
(18) </html>
(19) </body>
```

2. 请根据网页显示的效果图(图 4.6)和网页中的元素说明, 将 HTML 文本中 (n) 处的解答填入对应的答案栏中。

【说明】

序号	类型	说明
(1)	网页标题	文本: "Form 表单示例"
(2)	表单对象	Name: "frmLogin" method: "post" action: "login.aspx"
(3)	输入文本框	Name: "txtUser" Id: "txtUser"
(4)	文本标签	Label: class: "style1" 文本: "密 码"
(5)	复选框	Checkbox: checked name: ccm

这是一个简单的 HTML 文档, 显示的是一个网页列表信息, 显示界面如图 4.6 所示。

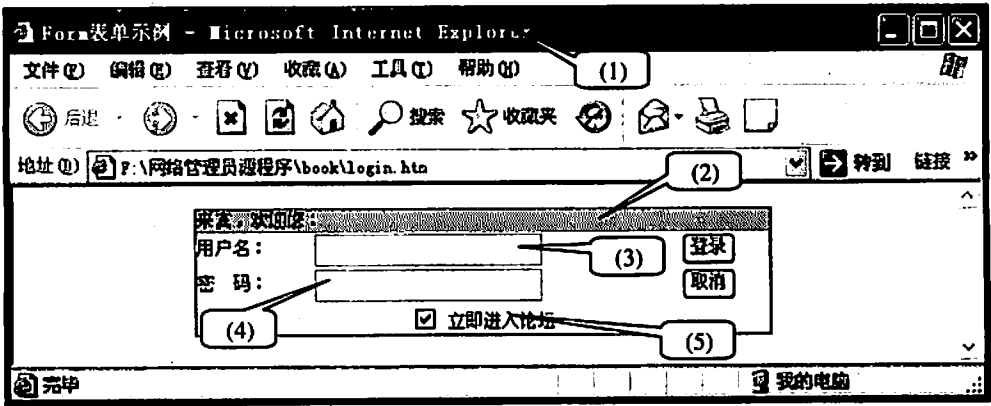


图 4.6 论坛网页

下面是这个论坛页面的 HTML 代码:

```
<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01 Transitional//EN"
"http://www.w3.org/TR/html4/loose.dtd">
<html>
<head>
<meta http-equiv="Content-Type" content="text/html; charset=gb2312">
(1)
<style type="text/css">
<!--
.style1 {
font-family: "宋体";
font-size: 12px;
```



```

}
-->
</style>
</head>
<body>
    (2)
    <table width="200" border="1" align="center" cellpadding="0"
    cellspacing="0" bordercolor="#CC9900">
        <tr>
            <td>
                <table width="381" border="0" align="center" cellpadding="0"
                cellspacing="0" bordercolor="#D4D0C8">
                    <tr>
                        <td colspan="3" bgcolor="#CCCC00" scope="col"><span class="style1">
来宾, 欢迎您: </span></td>
                    </tr>
                    <tr>
                        <td scope="col"><label class="style1">用户名: </span></label></td>
                        <td scope="col">_____(3)_____/td>
                        <td scope="col"><div align="left">
                            <input name=btnLogin type=submit id="btnLogin" style="FONT-SIZE:
12px" value=登录>
                        </div></td>
                    </tr>
                    <tr>
                        <td>_____(4)_____/td>
                        <td><input name="txtPasswd" type="text" id="txtPasswd"></td>
                        <td><input name=btnLogin type=submit id="btnLogin" style="FONT-SIZE:
12px" value=取消></td>
                    </tr>
                    <tr>
                        <td colspan="3"><div align="center" class="style1">
                            _____(5)_____
                            立即进入论坛</div></td>
                    </tr>
                </table>
            </td>
        </tr>
    </table>
</form>
</body>
</html>

```

#### 4.1.4 同步练习参考答案

1.

- (1) 第(7)行不正确: <title>标签必须位于<head>与</head>标签之间。
- (2) 第(9)行不正确: </strong>标签必须位于<p>与</p>之间。

- (3) 第(13)、(14)行位置不正确: 根据图像分析, 应将(13)、(14)行互换。
- (4) 第(17)行不正确: `<p>`之前的 `webmaster@yahoo.com.cn` 应置于`</a>`之前。
- (5) (18)、(19)行位置不正确: 根据图像分析, 应将(18)、(19)行互换。

2.

- (1) `<title>Form 表单示例</title>`
- (2) `<form name="frmLogin" method="post" action="login.aspx">`
- (3) `<input name="txtUser" type="text" id="txtUser">`
- (4) `<label class="style1">密 码: </label>`
- (5) `<input type="checkbox" checked="checked" name="csm">`

## 4.2 网页制作工具

### 4.2.1 考点辅导

网页制作工具主要是指所见即所得的 HTML 标签处理工具, 常用的网页制作工具有 Flash、Fireworks、Dreamweaver、Photoshop 和 FrontPage 等。

#### 4.2.1.1 Flash 简介

##### 1. Flash 概述

Flash 是 Macromedia 公司出品的一个网页交互式动画制作工具软件, 用它制作的 Flash 矢量动画图像清晰、文件体积小, 可以边下载边播放, 是网络流媒体的最佳选择之一。它的主要版本包括 Flash5、Flash MX 和 Flash MX 2004, 其中 Flash MX 2004 是它的最新版本。它包含 Macromedia Flash 的所有特点及功能, 另外还有很多高端特点, 比如数据源综合功能、支持专业视频、制作更神奇的应用程序及互动内容。

##### 2. Flash 工作环境

图 4.7 所示为 Flash MX 2004 的集成开发环境。

##### (1) 菜单栏

Flash MX 2004 的菜单栏共计有 10 个主菜单, 用于分类放置各种命令, 它们是:【文件】、【编辑】、【视图】、【插入】、【修改】、【文本】、【命令】、【控制】、【窗口】和【帮助】。在菜单栏中可以完成 Flash MX 2004 所有的命令操作, 其快捷键可以使用户更方便地操作使用。

##### (2) 工具栏

Flash MX 2004 的菜单栏下面一行是标准工具栏, 使用标准工具栏可以快捷地实现各种基本的编辑和修改操作。

##### (3) 时间轴

时间轴在标准工具栏之下, 主要用来组织 Flash 影片播放的顺序和控制影片内容在一定时间内播放的层数和帧数。时间轴的主要组件是图层、帧、播放头、图层控制和时间

线等。

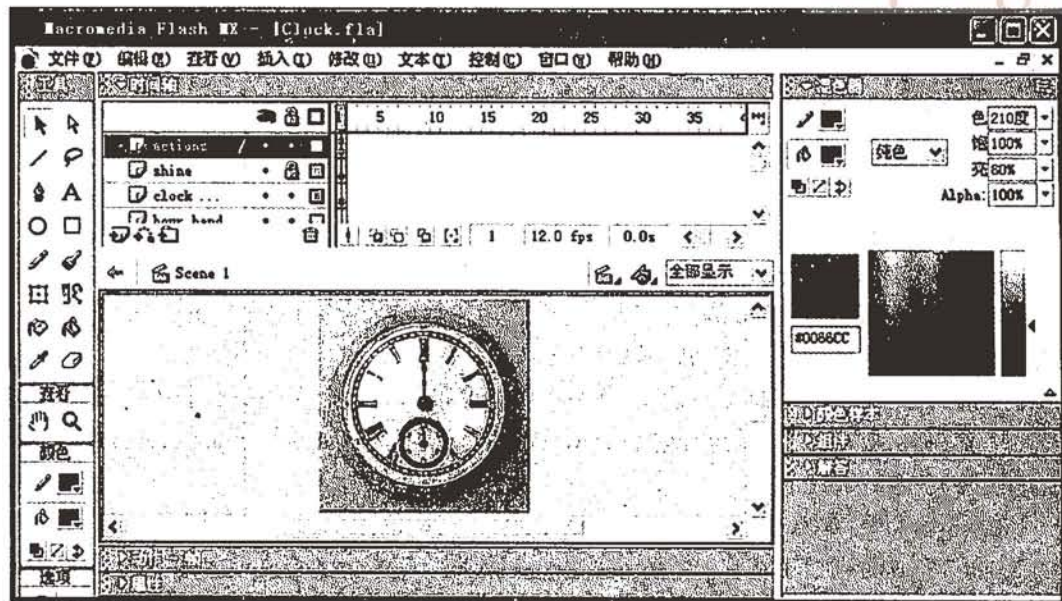


图 4.7 Flash MX 2004 集成开发环境

#### (4) 工具箱

工具箱是 Flash 的主要影片制作工具，其中放置了可供图形和文本编辑的各种工具，利用这些工具可以进行绘图、选取、喷涂、修改以及文字编辑等。

#### (5) 舞台

舞台也就是工作区，它是 Flash 的最主要的可编辑区域，在这里可以进行创作、修改、编辑动画对象，以及生成电影作品。

#### (6) 各种面板

Flash 的 IDE 环境包括属性、动作、混色器、行为和帮助等各种面板，面板提供了各种编辑和修改动画的相关操作。

### 3. Flash 的特点

(1) 可进行矢量图形处理。Flash 允许创建压缩的矢量图形，并使它“动”起来。同时，Flash 还允许输入或者模拟由其他程序生成的矢量图形和点阵图。

(2) 采用流播放技术。Flash 采用的流播放技术使得动画可以边播放边下载，从而节省了时间，避免了网页浏览者的焦急等待。

(3) 文件占用的存储空间小。Flash 通过使用关键帧和图符(元件)使得所生成的动画文件非常小。关键帧之间的帧序列由 Flash 自动生成。Flash 只保存图符的一份副本，因而可以减小文档的尺寸。Flash 的图符分为图形、按钮和电影片断 3 个类别。

(4) 具有强大的动画编辑功能。通过 Action 和 Fs Command，可以实现实时交互性，使 Flash 动画设计具有更大的设计自由度。另外，通过与主流的 Web 网页设计工具 Dreamweaver 的默契配合，可以将 Flash 影片嵌入到网页的任一位置，非常方便。

(5) 可使音乐、动画和声效融合一体。Flash 支持网络上主流的多种视频和音频格式。

在视频方面,支持 Quick Time(\*.mov)、数字视频(\*.dv, \*.dvi)、MPEG(\*.mpg, \*.mpeg)、Windows 视频(\*.avi)、Windows Media(\*.asf, \*.wmv)和 Macromedia Flash(\*.flv)等多种视频;在音频方面支持 WAV(\*.wav)、MP3(\*.mp3)、AIFF(\*.aif)和 Sun Au(\*.au)等多种音频。可以导入各种视频和音频,编辑和修改后能够生成高质量的 Flash 影片。

#### 4.2.1.2 Fireworks 简介

##### 1. Fireworks 概述

Fireworks 是 Macromedia 公司出品的一种专门针对 Web 图像设计的软件。在网页制作方面 Fireworks 不仅可以生成静态图像,还可以直接生成包含 HTML 和 Java Script 代码的动态图像以及其他各种交互式动感效果图像。

Fireworks 可使用户插入、编辑以及整合包括像素和矢量在内的所有的主流图形格式,快速创建图形和交互效果,轻松地把 Fireworks 图形输出到 Flash、Dreamweaver 以及第三方的应用程序。

Fireworks 的最新版本是 Fireworks MX 2004,它在位图编辑、矢量图形处理与 GIF 动画制作功能等方面进行了优化整合,加入了新的绘图工具与特效,同时具有完整的 Unicode 双字节支持,是网页图像制作的利器。

##### 2. Fireworks 的工作环境

图 4.8 所示为 Fireworks MX 2004 的集成开发环境。

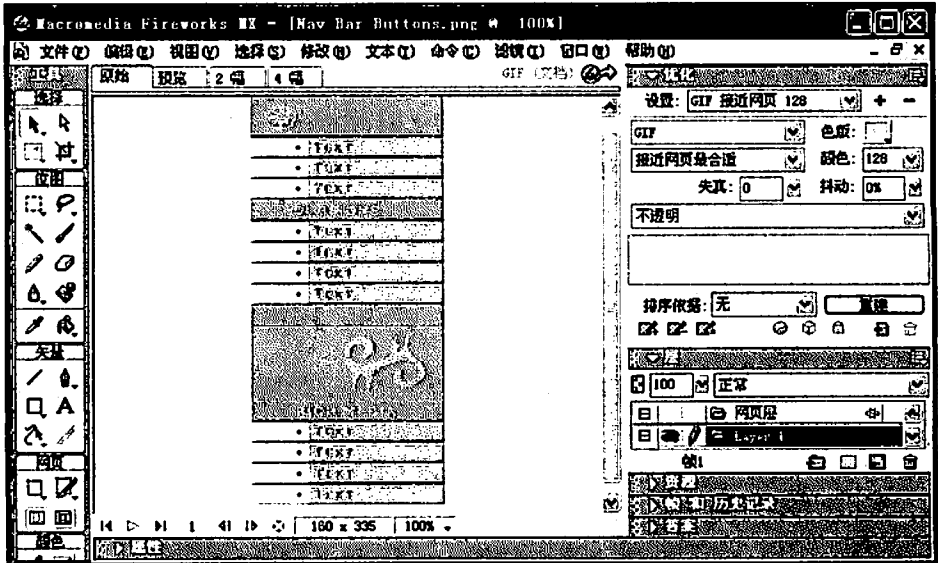


图 4.8 Fireworks MX 2004 集成开发环境

Fireworks MX 2004 的集成开发环境与 Flash MX 2004 风格一致,主要包括菜单栏、工具箱、文档窗口和各种面板等。

##### (1) 文档窗口

Fireworks 的文档窗口上有原始、预览、2 幅预览和 4 幅预览 4 个标签。可以同时编辑和预览图像,可以同时预览 4 种不同优化设置所产生的效果,并选择最理想的一种设定输



出图像。

## (2) 工具箱

工具箱中包括选择工具、位图工具、矢量工具、颜色工具、Web 工具和视图工具等工具集。利用相应的工具，可以选择、创建、编辑图像。

## (3) 矢量模式与位图模式

Fireworks 可以进行矢量模式与位图模式的编辑。默认状态下，Fireworks 打开时处理位图模式，可以利用工具箱中的位图或矢量工具绘制相应的图像。

## (4) 各种面板

Fireworks 包括各种浮动面板，主要有属性、优化、混色器、行为、层和库等。可以通过窗口菜单控制各种面板的显示和隐藏。

## 3. Fireworks 的特点

(1) 采用图像映像技术，显示效果好。图像映像是 Web 中经常使用的一种技术，它可以将一幅完整的图像在逻辑上分割为不同的区域(热区)，通过编码为每个热区指定不同的链接，跳转到不同的 URL 地址。这种方式不会造成图像的视觉割裂，显示效果较好。

(2) 采用切片技术，获得较高的下载速度。利用切片技术可以将一幅大图像真正分割为多个较小的图片，以获得较高的下载速度。在网页中，这些小图片被放置在 HTML 表格的不同单元格里，视觉上以一幅完整的图片显示。Fireworks 提供了定位参考线和切片工具，帮助分割图像，并且根据图像切片的大小，自动构建 HTML 表格。

(3) 构建按钮和轮替图像。在 Fireworks 中，可以快速构建多种风格的按钮，按钮编辑器可以快速高效地构建 Java Script 轮替图像按钮，还可以构建包含多个按钮的导航条。

(4) 样式特性，快速定制图像风格。利用 Fireworks 提供的样式特性，可以为图像快速应用一些设置好的艺术效果，例如可以设置图像的投影、发光和浮雕以及文字的纹理材质和三维效果等。

(5) 功能强大的图像优化特性。在 Fireworks 的工作环境中，可以对每个切片进行优化，以不同的图像文件格式进行存储。

除了上述的特点之外，Fireworks 还具有支持符号、实例和插帧等特点，以供用户方便地创建各种图像和动画。

### 4.2.1.3 Dreamweaver 简介

#### 1. Dreamweaver 概述

Dreamweaver 是 Macromedia 公司推出的一个所见即所得的主页编辑工具，是针对专业网页开发者的可视化网页设计工具。

在 Dreamweaver 中，几乎所有的网页对象均可在属性面板上进行修改。翻转图片、导航按钮、E-mail、日期、Flash 动画、Shockwave 动画和 Java Applet 等对象也可以通过对象面板插入到网页中。Dreamweaver 支持进行网站及应用内容的创建——可以是手写代码方式，也可以是所见即所得的页面编辑方式，或是两种模式并用，并且可以是在自己选定服务器端的技术支持之下，从而可以快速开发基于网络的 Web 应用程序。

目前的最新版本是 Dreamweaver MX 2004，Dreamweaver MX 2004 使得用户完成网络

及应用内容的开发创建易如反掌，并可以无限扩展用户的能力。

2. Dreamweaver 的工作环境

图 4.9 所示为 Dreamweaver MX 2004 的集成开发环境。

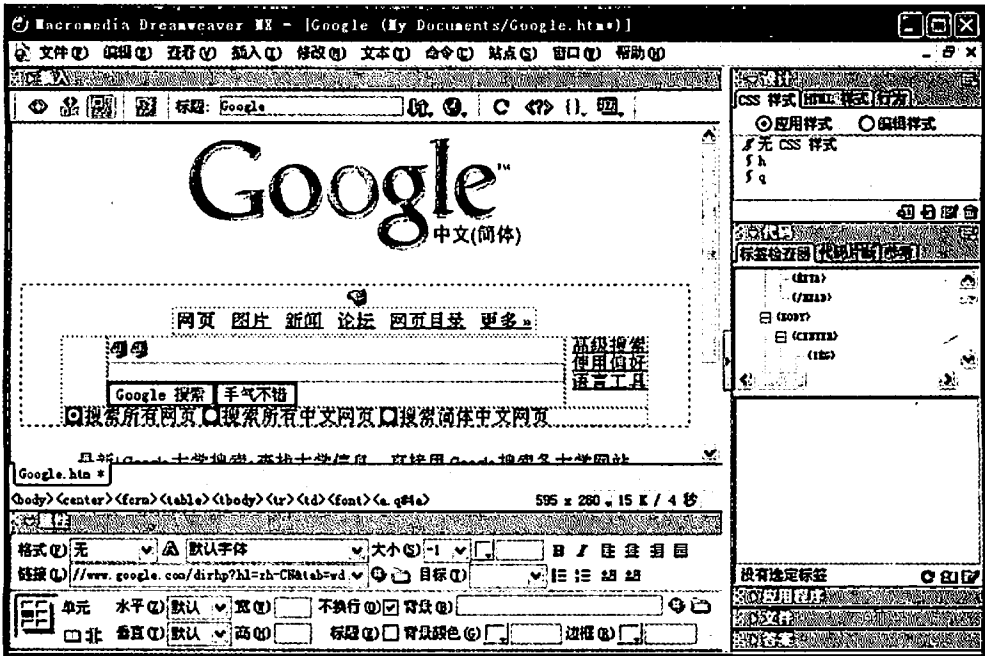


图 4.9 Dreamweaver MX 2004 集成开发环境

启动后的 Dreamweaver 由许多窗口组成，主要包括主菜单、文档工具栏、属性面板、对象面板和其他浮动面板。

(1) 主菜单

Dreamweaver 的主菜单共分为 10 大类：【文件】、【编辑】、【查看】、【插入】、【修改】、【文本】、【命令】、【站点】、【窗口】和【帮助】，主要提供网页编辑、站点管理和联机帮助等功能。

(2) 文档工具栏

文档工具栏能够提供网页视图切换、文件管理和预览调试等功能。

(3) 属性面板

属性面板随选择对象而变，主要用于分类设置相关对象的外观和其他参数。

(4) 对象面板

对象面板集成了主菜单中【插入】菜单的选项。

(5) 其他浮动面板

集成开发环境窗口中还可以根据需求打开设计、代码、应用程序和文件等其他浮动面板，能对网页设计提供帮助。

3. Dreamweaver 的特点

(1) 可视化开发与 HTML 源码的完美结合

Dreamweaver 提供可视化网页开发,同时不会降低 HTML 的源码控制,可以方便地实现现代码和设计视图的切换。

#### (2) 支持跨浏览器 DHTML 和其他动态元素

Dreamweaver 支持 Dynamic HTML、层叠样式单、绝对坐标定位和 Java Script 的动画。

#### (3) 提供行为和时间轴

Dreamweaver 为进行动画交互行为提供交互方式,其时间轴支持视频操作方式编辑网页。

#### (4) 与 Macromedia 其他软件的完美协作

Dreamweaver 中可以直接插入从 Fireworks 中导出的 HTML 代码,Dreamweaver 中的图像也可以直接使用 Fireworks 进行编辑和优化。

### 4.2.1.4 Photoshop 简介

#### 1. Photoshop 概述

Photoshop 是 Adobe 公司推出的一款功能十分强大、使用范围广泛的平面图像处理软件。Photoshop 具有广泛的兼容性,采用开放式结构,能够外挂其他处理软件和图像输入输出设备。利用它可以任意设计、处理和润饰各种图像,是美术设计、摄影和印刷专业人员理想的数字图像处理工具软件。

Adobe Photoshop CS 是 Adobe 公司出品的最新版本的 Photoshop,CS 实际上是 Creative Suit 的简单。Photoshop CS 新增了许多强有力的功能,特别是对于摄影师来讲,它大大突破了以往 Photoshop 系列产品更注重平面设计的局限性,对数码暗房的支持功能有了极大的加强和突破。

#### 2. Photoshop 的工作环境

图 4.10 所示为 Adobe Photoshop CS 的集成开发环境。

启动后的 Adobe Photoshop CS 集成开发环境,主要包括菜单栏、图像窗口和控制面板等。

##### (1) 菜单栏

菜单栏显示的是 Photoshop 菜单命令。包括【文件】、【编辑】、【图像】、【图层】、【选择】、【滤镜】、【视图】、【窗口】和【帮助】9 个菜单。

##### (2) 工具箱

工具箱列出了 Photoshop 中的常用工具。利用工具箱中的工具可以选择、绘制、编辑和查看图像,选择前景和背景色,以及修改屏幕显示模式。

##### (3) 图像窗口

图像窗口主要用于显示图像。窗口上方显示图像文件的名称、大小比例和色彩模式等。

##### (4) 控制面板

控制面板列出了 Photoshop 中许多操作的功能设置和参数设置,利用这些设置可以对文档窗口中的图像对象进行各种操作。

#### 3. Photoshop 的特点

##### (1) 支持多种图像格式

Photoshop 支持的图像格式包括 PSD、EPS、DCS、TIF、JPEG、BMP、PCX、FLM、



PDF、PICT、GIF、PNG、IFE、FPX、RAW 和 SCT 等 20 多种, 利用 Photoshop 可以进行图像格式的转换。

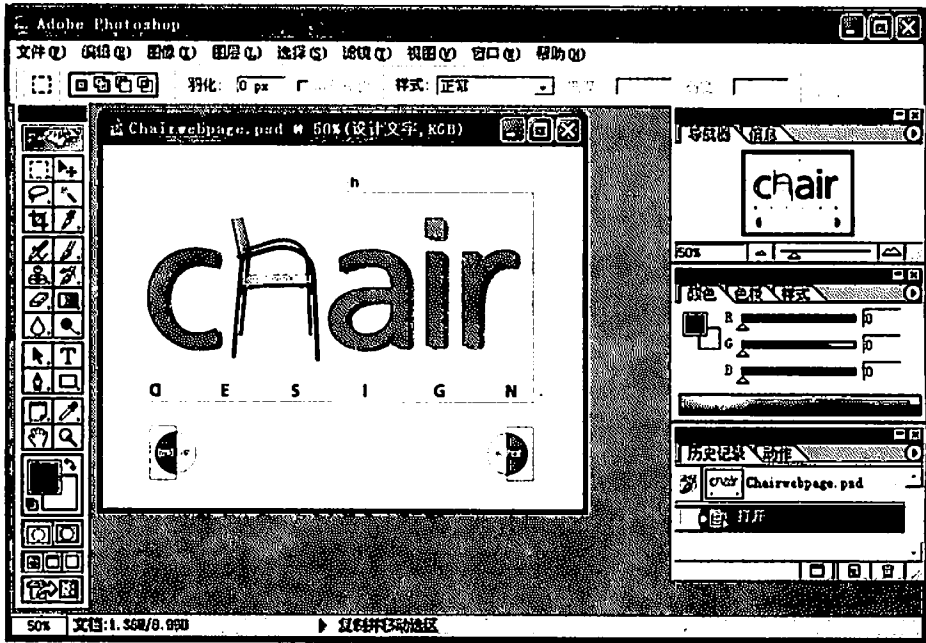


图 4.10 Adobe Photoshop CS 集成开发环境

#### (2) 支持多种色彩模式

Photoshop 支持的色彩模式包括位图模式、灰度模式、RGB 模式、CMYK 模式、LAB 模式、索引颜色模式、双色调模式和多通道模式等, 并且可以实现各种模式之间的转换。

#### (3) 强大的图像选取功能

利用矩形、椭圆面罩和套索工具, 可以选取不同大小、形状的选取范围。配合多种快捷键的使用, 可以实现选取范围的相加、相减、交叉和反选等效果。

#### (4) 支持图像各种编辑

在 Photoshop 中, 可以对图像进行各种编辑, 如复制、粘贴、剪切和消除, 还可以对图像进行任意的旋转和变形等。

#### (5) 支持图像色调色彩调整

Photoshop 可以对图像进行色调和色彩的调整, 也可以单独对某一选取范围或某一种选定颜色进行调整。

#### (6) 提供绘画功能

可以使用喷枪、笔刷、铅笔、直线绘制各种图形, 通过自行设定的笔刷形状、大小和压力, 创建不同的笔刷效果。还有渐变工具、加深和减淡工具、海绵工具以及模糊、锐化和涂抹等工具可以对图像进行编辑。

#### (7) 便捷的图层功能

使用 Photoshop, 用户可以建立和编辑普通层、背景层、文本层和调节层等多种图层。用户可以对图层进行任意的复制、移动、删除、翻转、合并和合成等。



### (8) 功能强大的滤镜功能

Photoshop 共提供了将近 100 种滤镜。用户可以利用这些滤镜实现各种特殊效果,如风、浮雕和水波效果等。

### 4.2.1.5 FrontPage 简介

#### 1. FrontPage 概述

FrontPage 是一款微软推出的专业 HTML 编辑器,它的最新版本是 FrontPage 2003,属于 Office 2003 的套件之一,主要用于对 Web 站点、Web 页面和 Web 应用程序进行设计、编码和开发。

#### 2. FrontPage 的工作环境

图 4.11 所示为 FrontPage 2003 的集成开发环境。

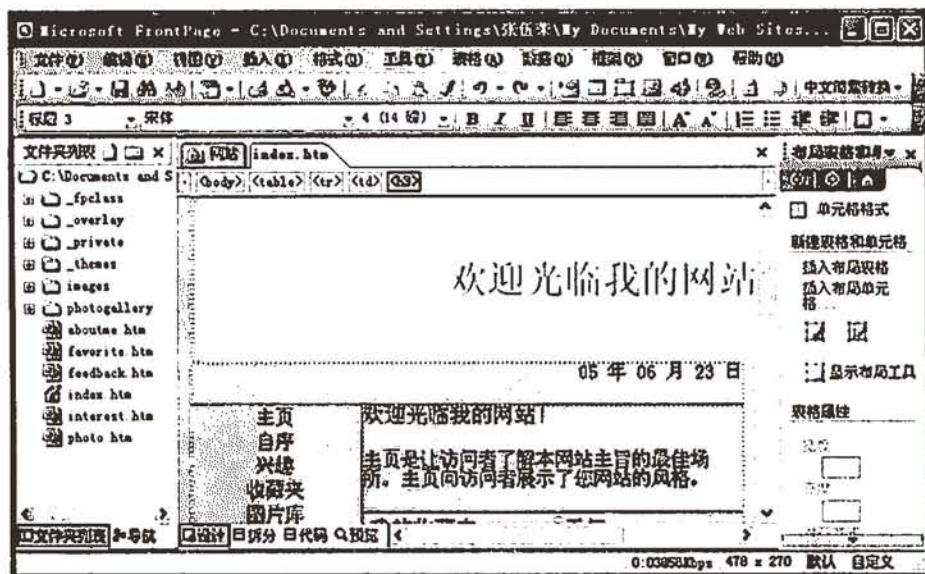


图 4.11 FrontPage 2003 集成开发环境

启动后的 FrontPage 2003 集成开发环境,主要包括菜单栏、工具栏和网页编辑区域等等,具体操作与 Office 中的 Word 软件类似。

#### 3. FrontPage 2003 的特点

(1) FrontPage 2003 提供了功能增强的设计环境,新的布局和设计工具、模板,以及改进的主题,主要包括动态 Web 模板、布局表格、单元格和支持 Macromedia Flash 等。

(2) FrontPage 2003 提供了一个功能增强的创作环境,具有新的图形功能,规则的 HTML 以及更多基于代码的控件。此外,其功能强大的编码工具有助于应用已掌握的各种编码语言知识,并帮助增强这方面的知识,以创建交互式脚本。内容主要包括拆分视图、智能感知和 ASP.NET 控件等。

(3) FrontPage 2003 以一种全新的方式使网站能够更方便地与其他人和信息进行连接。Microsoft Windows Server 2003 与 Microsoft Windows SharePoint Services 的结合使用可

以连接、编辑和展示来自多种数据源的实时数据——包括 Windows SharePoint Services 数据、XML、Web 服务以及 OLE DB 数据源——从而在所见即所得的编辑器中创建内容丰富、交互式的数据组织的网站。

### 4.2.2 典型例题分析

**例** 请回答以下关于 FrontPage 使用与操作的问题 1~4，把解答填入对应的答案栏内。  
(2001 年下午试题三)

**【问题 1】**

FrontPage 中的“字幕”效果有哪 3 种表现形式？

**【问题 2】**

当页面过长时浏览器会出现垂直滚动条，上下拖动滚动条会使页面背景图片也随之上下移动。为了使背景固定而不随滚动条上下移动，可以在【格式】菜单上的【背景】菜单项中选择哪一个选项来解决该问题？

**【问题 3】**

在所编辑的页面中插入图片，选中该图片，然后单击【格式】菜单中的【定位】菜单项，并选择【绝对定位】。这项操作的作用是什么？

**【问题 4】**

HTML 源代码段如下：

```
<body>
<table border = 1>
<tr>
<td>单元格一</td>
<td 单元格二</td>
<td>单元格三</td>
</tr>
<tr>
<td>单元格四</td>
</tr>
<tr>
<td>单元格五</td>
<td>单元格六</td>
</tr>
</table>
</body>
```

请画出该段 HTML 代码在 FrontPage “普通”状态下的显示状态。

**分析：**本题主要考查 FrontPage 网页制作软件的基本技能和使用技巧。

FrontPage 中的字幕是一种能使文本来回滚动的活动元素，一般用来播放一些活动的信息，如新闻、通知等。“字幕”效果有 3 种表现形式，即滚动条、幻灯片、交替。在实际操作中，可以通过点击 FrontPage 中的【插入】菜单中的【组件】子菜单中的【字幕】菜单项来实现。

在编辑网页时,有时需要使用背景图片,为了使背景固定而不随滚动条上下移动,可以通过点击【格式】菜单上的【背景】子菜单中的【水印】来实现。图片在网页中有3种定位方式,即无定位、相对定位和绝对定位。网页图片的绝对定位的作用是利用光标可以任意拖动图片,并可放置在页面的任何一个位置。

表格一般由标题、表头和表格数据组成。表格的 HTML 标记由

答案:

【问题1】3种效果的表现形式分别为滚动条、幻灯片、交替。

【问题2】水印。

【问题3】可以使用鼠标来移动这个图形。

【问题4】显示状态如图4.12所示。



图 4.12 表格显示状态

### 4.2.3 同步练习

请回答以下关于 Dreamweaver 使用与操作的问题 1 至问题 4,把解答填入对应答案栏内。

【问题1】Dreamweaver【插入】菜单下的【布局对象】子菜单包括哪几个对象?

【问题2】利用 Dreamweaver【新建】菜单,可以打开新建网页对话框,当选择建立动态网页时有许多选项,如 ASP JavaScript 和 ASP VBScript 文档,它们有何区别?

【问题3】利用 Dreamweaver 编辑网页时,可以创建网页文档之间的超级链接。目标网页的打开方式一般包括\_blank、\_parent、\_self、\_top,它们有何意义?

【问题4】HTML 源代码段如下:

```
<html>
<head>
<title>登录示例</title>
<meta http-equiv="Content-Type" content="text/html; charset=gb2312">
</head>
<body>
<br>
```

```

<form name="form1" method="post" action="">
  <table width="100%" border="0" cellspacing="0" cellpadding="1">
    <tr>
      <td> <table width="100%" border="0" cellspacing="0" cellpadding="4">
        <tr>
          <td width="20%" class="TitleColor">
            <label for="username"><strong>用户名</strong></label> <br>
            <input id="username" name="username" type="text" size="25">
            <p></p>
            <label for="password"><strong>密 码</strong></label><br>
            <input id="password" name="password" type="password" size="25">
            <p>
              <input type="submit" name="ButtonName" value="登录">
            </p></td>
        </tr>
      </table></td>
    </tr>
  </table>
</form>
</body>
</html>

```

请画出该段 HTML 代码在 IE 下的显示状态。

#### 4.2.4 同步练习参考答案

【问题 1】布局元素有 4 个对象，分别是 Div 标签、层、布局表格和布局单元格。

【问题 2】ASP JavaScript 是用 JavaScript 编写的 Active Server Pages 文档；ASP VBScript 是用 VBScript 编写的 Active Server Pages 文档。

【问题 3】\_blank 是将链接网页文档载入到新的未命名的浏览器窗口中；\_parent 将链接网页文档载入到父框架集或包含链接的框架窗口中；\_self 是将链接网页文档载入到同一框架或窗口中；\_top 是将链接网页文档载入到整个浏览器窗口并删除所有框架。

【问题 4】显示状态如图 4.13 所示。

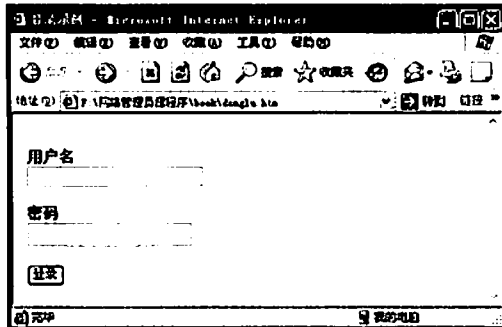


图 4.13 登录显示状态



## 4.3 动态网页制作

### 4.3.1 考点辅导

动态网页技术主要依赖服务器端编辑,包括 CGI 版本、Server-API 程序(NSAPI 和 ISAPI)、JavaServerlets 以及服务器脚本语言。

服务器脚本环境有许多,其中最流行的几种包括 ASP(Active Server Pages)、ASP.NET(基于 .NET 架构的 ASP)、JSP(Java Server Pages)、ColdFusion 和 PHP 等。

#### 4.3.1.1 ASP

##### 1. ASP 简介

###### (1) 什么是 ASP

ASP 是 Active Server Pages(动态服务器页面)的缩写,ASP 可以混合使用 HTML、脚本语言以及组件来创建服务器端功能强大的 Internet 应用程序。ASP 使用 Microsoft 的 ActiveX 技术,它采用封装程序调用对象的技术,从而简化了编程并且加强程序间的协作。

###### (2) ASP 的特点

ASP 运行在服务器端时,ASP 不需要编译,可在服务器端直接执行,ASP 与浏览器无关。ASP 返回标准的 HTML 页面,浏览者查看页面源文件时,看到的是 ASP 生成的 HTML 代码,而不是 ASP 程序代码。

###### (3) ASP 的编程环境

ASP 的编程语言可以是 VBScript 和 JavaScript,而 VBScript 则是系统默认的脚本语言。ASP 的编程语言可以使用普通的文本编辑器进行设计,ASP 程序则以扩展名 .asp 的纯文本形式保存在 Web 服务器上的具有可执行权限的虚拟目录之下,供用户通过 WWW 的方式访问。

##### 2. ASP 内嵌对象

ASP 提供了可以在脚本中使用的各种内嵌对象。这些内嵌对象主要用于收集浏览器请求信息、响应浏览器和存储用户的各种信息,从而简化编程工作。ASP 结构提供 6 个内建对象:Request、Response、Application、Session、Server 和 ObjectContext。内建对象的特殊性在于,它们在 ASP 页内生成且在脚本中使用它们前无须创建。

###### (1) Request 对象

Request 对象在 HTTP 请求期间,检索客户端浏览器传递给服务器的值。

其使用语法是:

```
Request[.collection|property|method](variable)
```

###### (2) Response 对象

用来访问服务器端所创建的并发回客户端的响应信息。

其使用语法是:

Response.collection|property|method

### (3) Application 对象

可以使用 Application 对象在给定的应用程序的所有用户之间共享信息。基于 ASP 的应用程序同所有的.asp 文件一样在一个虚拟目录及其子目录中定义。因为多个用户可以共享 Application 对象,所以必须要有 Lock 和 Unlock 方法以确保多个用户无法同时更改某一属性。

其使用语法是:

Application.method

### (4) Session 对象

可以使用 Session 对象存储特定用户会话所需的信息。这样,当用户在应用程序的 Web 页之间跳转时,存储在 Session 对象中的变量将不会丢失,而是在整个用户会话中一直存在下去。当用户请求来自应用程序的 Web 页时,如果该用户还没有会话,则 Web 服务器将自动创建一个 Session 对象。当会话过期或被放弃后,服务器将终止该会话。Session 对象最常见的一个用法就是存储用户的首选项。例如,如果用户指明不喜欢查看图形,就可以将该信息存储在 Session 对象中。

其使用语法是:

Session.collection|property|method

### (5) Server 对象

Server 对象提供对服务器上的方法和属性的访问。其中大多数方法和属性是作为实用程序的功能服务的。

其使用语法是:

Server.property|method

### (6)ObjectContext 对象

可以使用 ObjectContext 对象提交或放弃一项由 Microsoft Transaction Server (MTS) 管理的事务,它由 ASP 页包含的脚本初始化。

当 ASP 页包含@TRANSACTION 指令时,该页会在事务中运行,直到事务成功或失败后才会终止。

其使用语法是:

ObjectContext.method

## 3. ASP 使用范例

下面是一个 ASP 的简单示例:

```
<%@LANGUAGE="VBSCRIPT" CODEPAGE="936"%>
<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01 Transitional//EN"
"http://www.w3.org/TR/html4/loose.dtd">
<%
Dim weekstr(6)
```

```

weekstr(0) = "天" : weekstr(1) = "一"
weekstr(2) = "二" : weekstr(3) = "三"
weekstr(4) = "四" : weekstr(5) = "五"
weekstr(6) = "六"
Nweek = DatePart("w", Date() ) - 1
Cweek = weekstr(Nweek)
%>
<html>
<head>
<meta http-equiv="Content-Type" content="text/html; charset=gb2312">
<title>简单 ASP 文档</title>
</head>
<body>
<h2>星期<%=Cweek%>的水果是 </h2>
<hr>
<p align="center"> </p>
</body>
</html>

```

#### ASP 代码的相关说明:

ASP 是服务器脚本语言,所有的 ASP 命令都必须包含在<%和%>之内,例如:<%Dim weekstr(6)...%>。ASP 通过<%和%>中的表达式将执行结果输出到客户端浏览器。例如:<h2>星期<%=Cweek%>的水果是 </h2>,将前面获取的 Cweek 值发送到客户端,当变量 Cweek 的值是“三”时,在客户浏览器中显示结果如图 4.14 所示。



图 4.14 简单的 ASP 执行结果

#### 4.3.1.2 JSP

JSP(Java Server Pages)是由 Sun Microsystems 公司倡导,许多公司共同参与建立的一种动态网页技术标准。在传统的网页 HTML 文件(\*.htm,\*.html)中加入 Java 程序片段(Scriptlet)和 JSP 标签(tag),就构成了 JSP 网页(\*.jsp)。Web 服务器在遇到访问 JSP 网页的请求时,首先执行其中的程序片段,然后将执行结果以 HTML 格式返回给客户。程序片段可以操作数据库、重新定向网页以及发送 E-mail 等,这就是建立动态网站所需要的功能。所有程序操

作都在服务器端执行,网络上传送给客户端的仅仅是得到的结果,对客户端浏览器的要求最低,可以实现无 Plugin、无 ActiveX、无 Java Applet,甚至无 Frame。

### 1. JSP 的特点

JSP 与 ASP 和 PHP 相比有下列优点:

#### (1) 内容的生成和显示分离

使用 JSP 技术,Web 页面开发人员可以使用 HTML 或者 XML 标签来设计和格式化最终页面。还可以使用 JSP 标签或者小脚本来生成页面上的动态内容。

#### (2) 强调可重用的组件

绝大多数 JSP 页面依赖于可重用的、跨平台的组件(JavaBean 或 EJB)来执行应用程序所要求的更为复杂的处理。

#### (3) 采用标识简化应用开发

通过开发定制化标识库,JSP 技术是可以扩展的。第三方开发人员和其他人员可以为常用功能创建自己的标识库。

#### (4) 健壮性与安全性

由于 JSP 页面的内置脚本语言是基于 Java 编程语言的,而且所有的 JSP 页面都被译成 Java Servlet,所以 JSP 页面就具有 Java 技术的所有好处,包括健壮的存储管理和安全性。

#### (5) 良好的移植性

作为 Java 的一部分,JSP 拥有 Java 编程语言“一次编写,各处运行”的特点。

#### (6) 企业级的扩展性和性能

在与 Java 2 平台、J2EE 和 EJB 技术整合时,JSP 页面将提供企业级的扩展性和性能。

### 2. JSP 程序页面

下面是 JSP 的一个应用实例,主要完成日期对象的相关操作,首先获取系统当前时间,然后重新设置系统时间,将系统时间设置为北京 2008 年奥运会开始的时间。

```
<%@ page contentType="text/html; charset=GB2312" import = "java.util.*" %>
<HTML>
<HEAD>
<TITLE>日期对象各时间段的取得与设置</TITLE>
</HEAD>
<BODY>
<CENTER>
<FONT SIZE = 5 COLOR = BLUE>日期对象各时间段的取得与设置</FONT>
</CENTER>
<HR>
<P></P>
<%
//声明 Date 对象变量,并建立 Date 变量
Date date = new Date();
%>
当前系统日期为<Font color = red>
<%= date.getYear() + 1900%>/
```



```
<%= date.getMonth() + 1%>/  
<%= date.getDate()%>  
</Font><P></P>  
当前系统时间为<Font color = red>  
<%= date.getHours()%>:  
<%= date.getMinutes()%>:  
<%= date.getSeconds()%>  
</Font><P></P>  
<%  
date.setYear(108); //将年设置为 2008 年  
date.setMonth(7); //将月设置为 8 月  
date.setDate(8); //将日设置为 8 日  
date.setHours(8); //将小时设置为 8 时  
%>
```

重新设置的新时间为<Font color = red><%= date%></Font>是北京奥运会开始的时间。

```
</BODY>  
</HTML>
```

该 JSP 页面经过 JSP 服务器解释在客户浏览器上显示的结果如图 4.15 所示。



图 4.15 简单的 JSP 执行结果

### 3. JSP 技术的未来

JSP 技术被设计为一个开放的, 可扩展的建立动态 Web 页面的标准。通过与业界领袖的合作, SUN 保证 JSP 规范的开放性和可移植性, 可以使用任意客户机和服务器平台, 在任何地方编写和部署它们。将来, 工具供应商和其他厂商将通过为专门的功能提供客户化的标识库而扩展平台的功能。

#### 4.3.1.3 XML

XML 即 eXtensible Markup Language(可扩展标记语言)的缩写。XML 实际上是 Web 上表示结构化信息的一种标准文本格式, 同 HTML 一样, 都来自 SGML(标准通用标记语言)。

##### 1. XML 的特征

(1) XML 是元标记语言。HTML 定义了一套固定的标签, 有其特定的含义。XML 则

允许用户自己定义所需的标签。

(2) XML 描述的是结构和语义。XML 标签描述的是文档的结构和意义,而不是页面元素的格式。

(3) XML 文档的显示使用特有技术支持,例如通过样式单为文档增加格式化信息。

## 2. XML 基本语法

一个正规的 XML 文档由 3 个部分组成:一个可选的序言、文档的主体和可选的尾声。一个 XML 文档通常以一个 XML 声明开始,后面通过 XML 元素来组织数据。XML 元素包括标签和字符数据。

下面是一份格式正规的 XML 文档:

```
<?xml version="1.0" encoding="GB2312"?>
<?xml-stylesheet type="text/xsl" href="XslDemo01.xsl"?>
<!--以上是 XML 文档的序言部分-->
<BOOK>
<TITLE>Moby-Dick</TITLE>
<AUTHOR>
<FIRSTNAME>Herman</FIRSTNAME>
<LASTNAME>Melville</LASTNAME>
</AUTHOR>
<BINDING>hardcover</BINDING>
<PAGES>724</PAGES>
<PRICE>$9.95</PRICE>
</BOOK>
<!--以上是 XML 文档的主体部分,以下是文档的尾声部分-->
```

可以看出,XML 文档序言部分从文档的第一行开始,它可以包括 XML 声明、文档类型声明、处理指令等。文档的主体则是由文档根元素所包含的那一部分。XML 尾声部分在文档的末尾,它可以包含注释、处理指令或空白等。

## 3. 应用程序接口

XML 文档本身是一个文本文件,在需要访问文档中的内容时,需要 XML 解析器进行语法验证和提取内容。两个著名的 XML 解析器的标准规范分别是 W3C 标准组织制定的文档对象模型(DOM, Document Object Model)和 XML\_DEV 邮件列表成员定义的简单应用程序接口(SAX, Simple APIs for XML)。

XML 程序接口示意图如图 4.16 所示。

从图中可以看出,应用程序不是直接对 XML 文档进行操作,而是首先由 XML 解析器对 XML 文档进行分析,然后应用程序通过 XML 解析器所提供的 DOM 接口或 SAX 接口对分析结果进行操作,从而实现对 XML 文档的访问。

### (1) 文档对象模型(DOM)

在应用程序中,基于 DOM 的 XML 解析器将一个 XML 文档转换成一棵 DOM 树,应用程序通过 DOM 树来实现对 XML 文档数据的操作。DOM API 提供给用户的是一种随机访问机制。通过它,应用程序不仅可以在任意时候访问 XML 文档中的任何数据,而且可

以任意地插入、删除、修改和存储 XML 文档的内容。

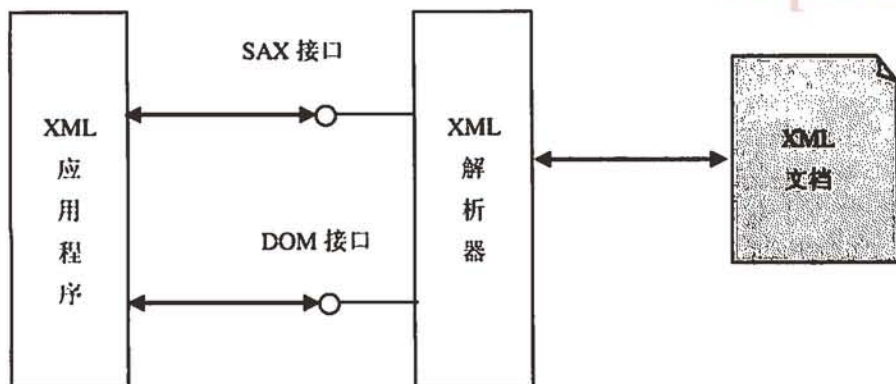


图 4.16 XML 程序接口示意图

DOM 解析器所采用的树形结构思想与 XML 文档结构吻合，应用十分广泛，但是对机器性能的要求较高，实现效率不是十分理想。

#### (2) 简单应用程序接口(SAX)

与 DOM 不同，SAX 采用的是顺序访问模式，是一种快速读写 XML 数据的方式。当 SAX 解析器对 XML 文档进行分析时，会触发一系列事件，并激活相应的事件处理函数，应用程序通过这些事件函数实现对 XML 文档的访问。同 DOM 解析器相比，SAX 实现简单，效率较高，但是缺乏灵活性，仅适用于访问 XML 数据，不适用于对文档进行更改的应用程序。

### 4. XML 文档的显示

由于 XML 中的标签许多是开发者自己定义的，主要用于说明文档所表述的数据的内存结构关系，因此其显示格式需要特殊的机制来定义。层叠样式单(CSS, Cascading Style-sheets)和扩展样式单语言(XSL, eXtensible Stylesheet Language)是 W3C 推荐的表达 XML 文档数据显示格式两种标准。

#### (1) 层叠样式单(CSS)

CSS 最初主要应用于 HTML 语言，可以保证文档显示格式的一致性和较好的格式化。通过 CSS 可以产生诸如字体、颜色和位置等不同样式的显示格式信息。CSS 可以存在于相应文档的页面中，也可以独立的文件形式存在，推荐使用独立的样式文件，以便于维护。CSS 在功能上不如扩展样式单语言强大，但是开发相对容易。

#### (2) 扩展样式单语言(XSL)

扩展样式单语言遵守 XML 的语法规则，是 XML 的一种具体应用。XSL 语言可以分为 3 个部分：转换工具(XSLT)、格式对象(FO)和 XML 分级命令处理工具 XPath。一个 XML 文档的显示过程是这样的：首先根据 XML 文档构造源树，然后根据给定的 XSL 将构造的源树转换为可以显示的结果树，最后按照 FO 解释结果树，产生一个可以在屏幕或其他媒体中输出的结果。

描述树转换的部分协议，已经从 XSL 中分离出来，取名为 XSLT。XSLT 的主要功能就是将源树转换为结果树。在 XSLT 中定义了与 XML 文档中各个逻辑成分相匹配的模板以

及匹配转换方式。具体的转换过程，既可以在服务器端进行，也可以在客户端进行。

下面是 XSLT 应用的一个简单例子。

```
XslDemo01.xml
<?xml version="1.0"?>
<!--File Name:XslDemo01.xml -->
<?xml-stylesheet type="text/xsl" href="XslDemo01.xsl"?>
<BOOK>
<TITLE>Moby-Dick</TITLE>
<AUTHOR>
<FIRSTNAME>Herman</FIRSTNAME>
<LASTNAME>Melville</LASTNAME>
</AUTHOR>
<BINDING>hardcover</BINDING>
<PAGES>724</PAGES>
<PRICE>$9.95</PRICE>
</BOOK>

XslDemo01.xsl
<?xml version="1.0"?>
<!--File Name:XslDemo01.xsl -->
<xsl:stylesheet xmlns:xsl="http://www.w3.org/TR/WD-xsl">
<xsl:template match="/">
<H2>Book Description</H2>
<SPAN STYLE="font-style:italic">Author:</SPAN>
<xsl:value-of select="BOOK/AUTHOR"/><BR/>
<SPAN STYLE="font-style:italic">Title:</SPAN>
<xsl:value-of select="BOOK/TITLE"/><BR/>
<SPAN STYLE="font-style:italic">Price:</SPAN>
<xsl:value-of select="BOOK/PRICE"/><BR/>
<SPAN STYLE="font-style:italic">Binding type:</SPAN>
<xsl:value-of select="BOOK/BINDING"/><BR/>
<SPAN STYLE="font-style:italic">Number of pages:</SPAN>
<xsl:value-of select="BOOK/PAGES"/>
</xsl:template>
</xsl:stylesheet>
```

在浏览器中查看到的浏览结果如图 4.17 所示。

#### 4.3.1.4 Java Script 和 VBScript

##### 1. Java Script

Java Script 是一种基于对象(Object)和事件驱动(Event Driven)并具有安全性能的脚本语言。使用它的目的是与 HTML 超文本标记语言、Java 脚本语言(Java Applet)一起实现在一个 Web 页面中链接多个对象，并与 Web 客户交互作用，从而可以开发客户端的应用程序等。它是通过嵌入在标准的 HTML 语言中实现的。它的出现弥补了 HTML 语言的缺陷，它是 Java 与 HTML 之间折衷的选择。





图 4.17 XML 文档在浏览器中的显示结果

## 2. VBScript

Microsoft Visual Basic Scripting Edition 是程序开发语言 Visual Basic 家族的最新成员, 它将灵活的 Visual Basic 应用于更广泛的领域, 包括 Microsoft Internet Explorer(IE)中的 Web 客户端脚本和 Microsoft Internet Information Server(IIS)中的 Web 服务器脚本。

### 4.3.2 典型例题分析

**例** 阅读下列说明和 HTML 文本, 分析其中嵌入的 Java Script 脚本, 将应填入\_\_\_\_(n) 处的语句写在对应的答案栏内。(2002 年网络程序员级下午试题四)

#### 【说明】

以下的 Java Script 脚本的功能是创建一个基于 resume 模型(表示简历)的对象 newguy(表示张春芳的简历), 并生成一个下拉列表框。该下拉列表框的选项是对象 newguy 的所有属性(如 name、sex 等)。用户在下拉列表框中选择了某个属性时, 就会打开一个新的浏览器窗口并输出该属性的值。例如, 若用户选择了 sex 属性时, 则会在浏览器窗口中输出: 您查阅的属性为 “sex”, 其值为 “女”。

一个下拉列表框的 HTML 文法如下例:

```
<select size="1" name="example">
  <option value="1">选项一</option>
  <option value="2">选项二</option>
</select>
```

下拉列表框的每一个选项都由 option 与 value 两部分组成, option 为用户可见的选项信息, value 为该选项的值。在 JavaScript 中, 该下拉列表框是一个对象, option 数组是该对象的属性。在上例中, example.option[1].text 的值为 “选项一”, 而 example.option[1].value 的值为 “1”。

#### 【HTML 文本】

object.html 中的内容为:

```
<html><head><title>对象的创建与使用</title>
<script language="JavaScript">
```

```

<!--
function printvalue() {
    var print_string="";
    for(__(1)__) {
        if (prop !='printvalue') //方法 printvalue 不能作为属性显示
            print_string=print_string+"<option value='" &
                +this[prop]+'>"+prop+"</option>";
    } //形成下拉列表框 option 部分的 HTML 文法字符串
    return print_string;
} //该函数用于产生下拉列表框 option 部分的 HTML 文法字符串
__(2)__ resume (name,sex,address,phone) {
    this.name=name; this.sex=sex;
    this.address=address; this.phone=phone;
    //以上为初始化模型的各属性
    this.printvalue=__(3)__;
    //将 printvale 函数映射为 resume 的 printvalue 方法
} //声明一个新的对象模型 resume。该模型为个人简历，用于创建个人简历对象
function displayvalue(selobj) {
    var disp_string
    disp_string="您查阅的属性为'"+__(4)___+"'其值为'"+&
        __(5)___+"'; //产生字符串
    newwin=window.open("", "hello", ""); //打开新浏览器窗口
    __(6)___; //在新窗口中打开文档
    newwin.document.write(disp_string); //在文档中显示信息
}
--> </script></head>
<body>
<script language="JavaScript">
<!--
newguy=__(7)___("张春芳","女","北京朝阳路 57 号","010-67456789");
//创建一个新的 resume 对象，对象名称为 newguy
document.write("<form method='POST' action=''>");
document.write("<p><select onChange='displayvalue(this)' name='resume'
size='1'>");
//指定下拉列表框在选择改变时触发 displayvalue 函数
document.write(__(8)___); //输出列表框的 options 部分
document.write("</select></p></form>");
//利用对象 newguy 的方法 printvalue 产生该下拉列表框的 HTML 文法
-->
</script></body></html>

```

**分析：**本题主要考查考生对 Java Script 的用户自定义对象的创建、事件驱动编程方法和选择列表的应用。

Java Script 是面向对象的脚本语言，是以对象为中心进行程序设计的，Java Script 提供了以下 7 种内部对象：数组、布尔、日期、函数、数学、数值和字符串对象。建立自定义对象就是为对象定义属性和方法，其步骤为：写一个构造函数来定义对象类型，利用 new

关键字建立对象实例。

事件驱动编程方法的关键就是“事件”和“事件处理程序”。使用事件处理程序的语法有两种：将事件处理程序视为一种对象的属性，直接嵌入 HTML 的标签内；视事件处理程序为对象的属性，直接写在对象后面。

表单对象提供了让客户端输入文字或进行选择的功能。“选择列表”通常建立在“表单”中，是由<select>和<option>标签共同生成的。

答案：

- (1) var prop in this
- (2) function
- (3) printvalue
- (4) selobj.options[selobj.selectedIndex].text
- (5) selobj.options[selobj.selectedIndex].value
- (6) newwin.document.open( )
- (7) new resume
- (8) newguy.printvalue( )

### 4.3.3 同步练习

阅读下列说明和 HTML 文本，分析其中嵌入的 Java Script 脚本，将应填入 (n) 处的语句写在对应的答案栏内。

【说明】

在网页设计中，浏览器的状态栏中可以设置动态字幕，浏览器的标题栏也可以设置成动画。下面的 Java Script 代码主要用于实现浏览器的标题栏动画。

网页的显示效果如图 4.18 所示。



图 4.18 浏览器上方滚动的标题栏

【HTML 文本】

```
<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01 Transitional//EN"
"http://www.w3.org/TR/html4/loose.dtd">
<html>
    _____ (1) _____
    step=0
    function flash_title()
    {
```

```
        _____(2)_____
    if (step==3) {step=1}
    if (step==1) {document.title='☆全国计算机技术与软件专业技术资格(水平)考试办公室★'}
    if (step==2) {document.title='★欢迎您, 报考网络管理员水平考试! ☆'}
    _____(3)_____
}
_____ (4) _____
</script>
<head>
<meta http-equiv="Content-Type" content="text/html; charset=gb2312">
<title>滚动的标题栏文本</title>
</head>
<body>
请注意观察滚动的浏览器标题栏文本!
</body>
</html>
```

### 4.3.4 同步练习参考答案

- (1) <script language=JavaScript>
- (2) step++
- (3) setTimeout("flash\_title()",180);
- (4) flash\_title()

## 4.4 Web 网站的创建与维护

### 4.4.1 考点辅导

#### 4.4.1.1 Web 网站的创建

##### 1. 组织信息

创建 Web 网站时, 需要考虑网站的扩展性、网页技术和网页制作工具的选择, 同时还必须考虑网站信息分解、网页链接、主题列表和逻辑顺序等, 确保做好网站规划。

##### 2. 构建网站框架

构建网站框架时, 可以考虑采用布告板、单页线性、多页线性、分层和网状等逻辑组织形式以提高网站的编码效率。

##### 3. 建立 Web 服务器

##### (1) Web 服务器简介

Web 服务器是用来存储网页并响应执行用户的访问请求的设备。Web 服务器对通过因特网使用 HTTP 协议的文件、文件夹以及其他资源的访问进行管理。当前两种最流行的 Web



服务器是运行于 Linux 操作系统平台上的 Apache Web 服务器和运行于 Windows 操作系统平台上的 Microsoft 的 IIS Web 服务器。

获得 Web 服务器空间的方式主要包括企业或单位自建和托管 Web 主机两种方式。企业或单位安置服务器需要相应的硬件、软件，还需要相关的人员来架设并维护 Web 服务器。

## (2) IIS Web 服务器

利用 IIS 的主要功能可以设置个人 Web 服务器，在工作组中共享信息，访问数据库，开发企业 Intranet 和开发 Web 应用程序。

用户可以通过 Windows 的计算机管理控制台或通过编写脚本来管理 IIS。还可以使用控制台，通过 Web 与他人共享使用 Internet 信息服务管理的站点和服务器的内容。从控制台访问 Internet 信息服务器，可以配置最常用的 IIS 设置和属性。开发站点和应用程序之后，可以在运行功能更加强大的 Windows Server 环境中使用这些设置和属性。

## 4. 域名注册

域名解析服务器主要负责将 Web 或其他服务器域名解析为相应的 IP 地址。选择适当的域名后，就可以到中国互联网络信息中心进行注册域名，并签订相应的域名注册协议。

## 5. Web 网站发布

网站发布之前需要准备 Web 服务器的相关信息，主要包括 Web 服务器协议、URL 地址、服务器文件系统规则和服务器账号等。实施 Web 发布时，可以采用 FTP 工具将网站文件从本地传输到远程服务器上。

### 4.4.1.2 Web 网站的维护

#### 1. 网站维护

网站维护主要涉及网站系统平台维护和网站内容更新维护两个主要方面。

#### 2. 网站测试

网站测试的主要内容包括浏览器的可变性、不同的分辨率和链接的有效性等。

## 4.5 本章小结

本部分内容主要要求考生掌握 Web 网站建设的相关内容，包括 HTML 的基础知识，HTML 应用，网页制作工具使用，动态网页技术以及 Web 网站的建立、管理和维护等 Web 基础知识和应用实现等内容。

对 Web 网站建设的学习关键要充分掌握 HTML 的基础知识，以常用的 HTML 元素为主线，抓住重点，熟悉 Web 网站建设中的动态网页技术使用和网站管理与维护等相关内容。本章的每小节中组织了大量的针对水平考试的典型例题分析和同步训练，这些题目涵盖了大纲规定的知识要点。

## 4.6 达标训练题及参考答案

### 4.6.1 达标训练题

1. 要定义显示一个如图 4. 19 所示的网页表格，相关信息参考下面的【网页说明】。将 HTML 文本中 (n) 处的解答填入对应栏中。

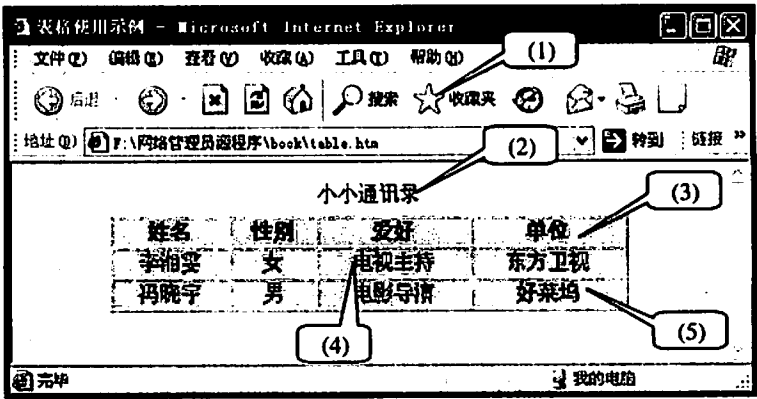


图 4. 19 表格在浏览器中打开的效果

【网页说明】

序号	类型	说明
(1)	网页标题	文本：“表格使用示例”
(2)	表格标题	文本：“小小通讯录”
(3)	单元格标题	内容：“单位” 对齐方式：居中
(4)	单元格内容	内容：“电视主持” 对齐方式：居中
(5)	表格结束	表格结束 HTML 标签

【HTML 文本】

```
<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01 Transitional//EN"
"http://www.w3.org/TR/html4/loose.dtd">
<html>
<head>
<meta http-equiv="Content-Type" content="text/html; charset=gb2312">
(1)
</head>
<body>
<table width="200" border="1" bgcolor="#CCCCCC" align="center">
(2)
<thead>
```

```

<tr>
  <th align="center">姓名</th>
  <th align="center">性别</th>
  <th align="center">爱好</th>
  _____
  (3)
</tr>
</thead>
<tbody>
<tr>
  <td align="center">李湘雯</td>
  <td align="center">女</td>
  _____
  (4)
  <td align="center">东方卫视</td>
</tr>
<tr>
  <td align="center">冯晓宇</td>
  <td align="center">男</td>
  <td align="center">电影导演</td>
  <td align="center">好莱坞</td>
</tr>
</tbody>
_____
(5)
</body>
</html>

```

2. 要定义一种用 Java Script 编写的在页面的固定广告位轮流播放广告的方法, 显示一个如图 4.20 所示的网页效果, 相关信息参考下面的【网页说明】。将 HTML 文本中 (n) 处的解答填入对应栏中。



图 4.20 轮流播放广告

【网页说明】

序号	类型	说明
①	定义初始变量	变量 i: i=1
②	设置 banner1 的图片源	图片源: pictures/yp.jpg
③	创建图片超级链接数组	数组名: links
④	设定窗口的状态条信息	状态条信息: description[i]
⑤	页面整体调入后, 开播广告	事件调用 startTime()

【HTML 文本】

```
<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01 Transitional//EN"
"http://www.w3.org/TR/html4/loose.dtd">
<html>
<head>
<meta http-equiv="Content-Type" content="text/html; charset=gb2312">
<title>动态广告链接</title>
<script language="JavaScript">
    <!-- Hide from old browsers
        (1) _____;
    banner1= new Image();
        (2) _____;
    banner2 = new Image();
    banner2.src = "pictures/aigo.jpg";
    banner3 = new Image();
    banner3.src = "pictures/lk.jpg";
        (3) _____;
    links[1] = "http://www.it168.com/digital/mp3.html"
    links[2] = "http://tech.tom.com/digital/mp3.html"
    links[3] = "http://www.163.com/digital/mp3.html"
    description = new Array
    description[1] = "IT168 数码—mp3 精品"
    description[2] = "TOM 科技—mp3 精品"
    description[3] = "网易数码—mp3 精品"
    function startTime(){
        var time= new Date();
        hours= time.getHours();
        mins= time.getMinutes();
        secs= time.getSeconds();
        closeTime=hours*3600+mins*60+secs;
        closeTime+=5;
        Timer();
    }
    function Timer(){
        var time= new Date();
        hours= time.getHours();
```



```

mins= time.getMinutes();
secs= time.getSeconds();
curTime=hours*3600+mins*60+secs
if (curTime>=closeTime){
  if (i <3){ // 图形总数
i++;
  document.banner.src = eval("banner"+i+".src");
}
else {
i = 1;
document.banner.src = eval("banner"+i+".src");
}
startTime();
}
else{
  window.setTimeout("Timer()",1000)}
}
function clickUrl(){
location.href = links[i]
}
function descript(){
  (4) _____;
}
//-->
</script>
</head>
<body _____ (5) _____;">
<center>
  <a href="http://www.it168.com" onClick="clickUrl(); return false;"
onMouseOver="descript(); return true;" onMouseOut="window.status=""></a>
</center>
</body>
</html>

```

## 4.6.2 参考答案

1.

- (1) <title>表格使用示例</title>
- (2) <caption>小小通讯录</caption>
- (3) <th align="center">单位</th>
- (4) <td align="center">电视主持</td>
- (5) </table>

2.

- (1) `var i = 1`
- (2) `banner1.src = "pictures/yp.jpg"`
- (3) `links = new Array`
- (4) `window.status = description[i]`
- (5) `onLoad="startTime( )"`

## 第5章 网络系统的运行、维护和管理

大纲要求:

- 使用网络管理软件对网络的配置、安全、性能、故障、计费进行监督和管理
- 简单网络故障的分析、定位、诊断和排除
- 小型网络的维护策略、计划和实施
- 数据备份和数据恢复
- 系统性能分析: 系统潜在问题分析

### 5.1 网络管理软件

#### 5.1.1 考点辅导

##### 5.1.1.1 网络管理系统

当前能够作为管理进程运行的典型的网络管理软件有: 惠普公司的 OpenView、IBM 公司的 NetView、SUN 公司的 SunNet 以及 Cabletron 公司的 SPECTRUM。这些网络管理系统都在支持企业网络管理方案的同时, 支持通过 SNMP 对网络对象进行管理。

##### 5.1.1.2 TCP/IP 网络管理工具

网络管理工具有连接性测试程序(ping)、路由跟踪程序(tracert/trace/traceroute)、协议统计程序(netstat)和 MIB 变量浏览器。

##### 1. ping: 验证与远程计算机的连接

连接性测试程序就是 ping, 是一种最常见的网络工具, 用这种工具可以测试端到端的连接性, 即检查源端到目的端网络是否通畅。ping 的原理很简单, 就是从源端向目的端发送一定数量的数据包, 然后从目的端返回这些数据包的响应, 如果在一定的时间内收到响应, 则程序返回从数据包发出到收到的时间间隔, 这样根据时间间隔就可以统计网络的延迟。如果在一定时间间隔内没有收到数据包的响应, 则程序认为数据包丢失, 返回请求超时信息。这样如果让 ping 一次发一定数量的包, 然后检查收到相应包的数量, 则可统计出端到端网络的丢包率, 而丢包率是检验网络质量的重要参数。

如果执行 ping 命令不成功, 故障可能出现在以下几个方面: 网线故障、网络适配器配置不正确、IP 地址不正确。如果执行 ping 命令成功而网络仍无法使用, 那么可以证实从源端到目的端之间所有物理层、数据链路层和网络层的功能都运行正常, 问题很可能出在网络系统的软件配置方面。因此, ping 命令成功只能保证本机与目标主机间存在一条连通的物理路径。

命令格式:

```
ping IP 地址或主机名 [-t] [-a] [-n count] [-l size]
```

参数含义:

-t: 指定在中断前 ping 可以持续发送回响请求信息到目的端。要中断并显示统计信息, 按 Ctrl+Break。要中断并退出 ping, 按 Ctrl+C。

-a: 指定对目的端 IP 地址进行反向名称解析。如果解析成功, ping 将显示相应的主机名。

-n count: 指定发送回响请求消息的次数, 具体次数由 count 来指定。若不指定次数, 则默认值为 4。

-l size: 指定发送的回响请求消息中“数据”字段的长度(以字节表示)。默认值为 32。size 的最大值是 65527 字节。

当计算机不能访问 Internet 时, 可以首先使用 ping 命令确认是否是本地局域网的故障。假定局域网的代理服务器 IP 地址为 202.168.0.1, 可使用 ping 202.168.0.1 命令查看本机是否和代理服务器连通。再测试本机的网卡是否正确安装, 常用命令是 ping 127.0.0.1。

## 2. tracert/trace/traceroute: 路由跟踪程序命令

路由跟踪程序命令在不同系统中的命令并不相同, 在 Windows 环境下使用 tracert 命令, 在 Linux 或 Unix 下使用 traceroute 命令, 在 Cisco 路由器中使用 trace 命令。

该诊断程序将包含不同生存时间(TTL)值的 Internet 控制消息协议(ICMP)回显数据包发送到目标主机, 以决定到达目标主机所经历的路由器。它要求路径上的每个路由器在转发数据包之前至少将 IP 数据包中的 TTL 递减 1。这样, TTL 就成为最大链路计数器。数据包上的 TTL 到达 0 时, 路由器应该将“ICMP 已超时”的消息送回源计算机。该程序首先发送 TTL 为 1 的第一条“回响请求”消息, 并在随后的每次发送过程将 TTL 递增 1, 直到目标响应或跃点达到最大值, 从而确定路径。

通过路由跟踪程序命令可以获得数据包从源主机到达目标主机所经过的路径, 并显示到达每个节点的时间。该工具主要有两个用途, 一是用来检测端到端是不是连通, 如不连通则找出问题出在哪儿。如果检查出到某一个路由器之前都能正常响应, 到这个路由器就不能响应了, 就很容易知道: 如果是线路出现故障, 故障点可能就出在这里。二是用来检查路由循环。如果在网络中某个路由器的路由配置不当, 导致路由循环, 使用该工具可以很方便地发现问题。如路由跟踪一端到另一端时, 发现到某一路由器之后, 出现的下一个路由器正是上一个路由器, 返回的结果在两个路由器之间来回交替出现, 这时往往是这个路由器的路由配置指向了前一个路由器, 导致路由循环了。

tracert 命令功能同 ping 类似, 但它所获得的信息要比 ping 命令详细得多, 可将数据包所经过的全部路径、节点的 IP 以及花费的时间都显示出来, 该命令比较适用于大型网络。

下面是 Windows 2000 环境下路由跟踪程序 tracert 的命令格式:

```
tracert [-d] [-h maximum_hops] [-j computer-list] [-w timeout] target_name
```

参数含义:

-d: 指定不将地址解析为计算机名。

-h maximum\_hops: 指定搜索目标的最大跃点数。



-j computer-list: 指定沿 computer-list 的稀疏源路由。

-w timeout: 每次应答等待 timeout 指定的毫秒数。

target\_name: 目标计算机的名称或 IP 地址。

例如想要了解自己的计算机与目标主机 www.cctv.com.cn 之间详细的传输路径信息, 可以在 MS-DOS 方式下输入 `tracert www.cctv.com.cn`。

如果我们在 `tracert` 命令后面加上一些参数, 还可以检测到其他更详细的信息, 例如使用参数 -d, 可以指定程序在跟踪主机的路径信息时, 同时也解析目标主机的域名。

### 3. netstat: 协议统计程序

`netstat` 命令可以帮助网络管理员了解网络的整体使用情况。它可以显示当前正在活动的网络连接的详细信息, 例如显示网络连接、路由表和网络接口信息, 可以统计目前总共有哪些网络连接正在运行。`netstat` 命令只有在安装了 TCP/IP 协议后才可以使

用。利用该命令的参数, `netstat` 命令可以显示所有协议的使用状态, 这些协议包括 TCP 协议、UDP 协议以及 IP 协议等, 另外还可以选择特定的协议并查看其具体信息, 还能显示所有主机的端口号以及当前主机的详细路由信息。

下面是 Windows 2000 中的 `netstat` 命令格式:

```
netstat [-a] [-e] [-n] [-s] [-p protocol] [-r] [interval]
```

参数含义:

-a: 显示所有连接和侦听端口。服务器连接通常不显示。

-e: 显示以太网统计。该参数可以与 -s 选项结合使用。

-n: 以数字格式显示地址和端口号(而不是尝试查找名称)。

-s: 显示每个协议的统计。默认情况下, 显示 TCP、UDP、ICMP 和 IP 的统计。-p 选项可以用来指定默认的子集。

-p protocol: 显示由 protocol 指定的协议的连接; protocol 可以是 tcp 或 udp, 如果与 -s 选项一同使用显示每个协议的统计, 则 protocol 可以是 tcp、udp、icmp 或 ip。

-r: 显示路由表的内容。

interval: 重新显示所选的统计, 在每次显示之间暂停 interval 秒。按 Ctrl+B 停止重新显示统计。如果省略该参数, `netstat` 将打印一次当前的配置信息。

### 4. MIB 变量浏览器

MIB 变量浏览器是另一种重要的网络管理工具。在 SNMP 中, MIB 变量包含了路由的几乎所有重要参数。对路由器进行管理, 很大程度上是利用 MIB 变量来实现的。比如, 路由器的路由表、路由器的端口流量数据、路由器中的计费数据、路由器 CPU 的温度、负载以及路由器的内存余量等, 所有这些数据都是从路由器的 MIB 变量中采集到的。虽然对 MIB 变量的定时采集与分析, 大部分都是程序进行的, 但一种图形界面下的 MIB 变量浏览器也是需要的。一般 MIB 变量浏览器, 都按照 MIB 变量的树形命名结构进行设计, 这样就可以自顶向下, 根据所要浏览的 MIB 变量的类别逐步找到该变量, 而无须记住该变量复杂的名字。网络管理人员可以利用 MIB 变量浏览器取出路由器当前的配置信息、性能参数以及统计数据等, 对网络情况进行监控。

Microsoft 提供了一个实用程序 Snmputil, 可以用于测试 SNMP 服务, 也可以用于测试用户开发的扩展代理。

Snmputil 的用法是:

```
Snmputil [get|getnext|walk] agentaddress community old[old...]  
Snmputil trap
```

可以使用 Snmputil 发送 GetRequest 或 GetNextRequest 报文, 也可以用 Snmputil 遍历整个 MIB 子树。一种较好的测试方法是同时打开两个 DOS 窗口, 在一个窗口中用 Snmputil 发送请求, 在另一个窗口中用 Snmputil 接收异常报告情况。

### 5.1.2 典型例题分析

**例 1** ping 是网络管理员最常用的一个网络工具, 它主要用于测试端到端的连接性。但我们经常使用“ping 127.0.0.1”、“ping <本机 IP 地址>”和“ping <默认网关 IP 地址>”, 而不直接使用“ping <远程主机 IP 地址或域名>”。请问这些命令分别有什么样的功能?

**分析:** 该题主要考查考生对 ping 命令使用掌握情况。

连接性测试程序 ping 主要用于测试端到端的连接性, 是网络故障排除时最常用的工具之一。当发现一台主机与另一台主机无法正常通信时, 第一步是 ping 环回地址(127.x.x.x)来验证在本地计算机上是否安装 TCP/IP 协议以及配置是否正确, 如果能 ping 通说明 TCP/IP 协议已经安装; 第二步是 ping 本地计算机的 IP 地址来验证本机是否被正确地添加到网络, 如果没有能则有可能与其他计算机的 IP 地址冲突或网卡安装不正确; 第三步是 ping 默认网关的 IP 地址验证默认网关是否运行以及能否与本地主机通信; 最后再 ping 远程主机的 IP 地址或域名来验证能否正常通信, 如果能通信, 则问题可能出现在网络系统的软件配置方面。

**答案:** 略

**例 2** 某一大型园区网, 由若干个路由器构成园区网主干。有两台 Windows 2000 主机无法正常通信, 我们怀疑是其中某个路由器工作不正确或配置错误而引起的, 网络管理员应用什么命令来找到这个路由器?

**分析:** 该题主要考查考生对 tracert 命令使用掌握情况。

在 Windows 2000 中提供了一个跟踪程序命令 tracert 可以跟踪数据包经过的路由。该工具将包含不同生存时间(TTL)值的 Internet 控制消息协议(ICMP)回显数据包发送到目标主机, 以决定到达目标主机所经历的路由器。由于要求路径上的每个路由器在转发数据包之前至少将 IP 数据包中的 TTL 递减 1, 所以 TTL 是有效的跃点计数。数据包上的 TTL 到达 0 时, 路由器应该将“ICMP 已超时”的消息送回源主机。路由跟踪程序先发送 TTL 为 1 的回显数据包, 并在随后的每次发送过程将 TTL 递增 1, 直到目标响应或 TTL 达到最大值, 从而确定数据包经过的路由器。如果检查出到哪个路由器之前都能正常响应, 到某一个路由器就不能响应了, 这样就很容易知道如果线路出现故障, 故障点就可能出在某处。

**答案:** tracert <目的主机的 IP 地址或域名>

**例3** 为了分析一台安装了 Windows Server 2003 服务器的网络流量,使用查看网络状态信息工具 netstat。如果想每 30 秒统计一下 TCP 连接情况,该使用哪些参数?(写出完整命令)

**分析:** 该题主要考查考生对 netstat 命令使用掌握情况。

netstat 命令可以帮助网络管理员了解网络的整体使用情况。它既可以显示当前正在活动的网络连接的详细信息,例如显示网络连接、路由表和网络接口信息,也可以统计目前总共有哪些网络连接正在运行。其命令格式为:

```
netstat [-a] [-e] [-n] [-s] [-p protocol] [-r] [interval]
```

其中参数-p protocol 用于显示指定协议的网络连接,参数-s 用于显示每个协议的统计,参数 interval 设定重新显示所选统计的间隔时间。因此命令为:

```
netstat -s -p TCP 30
```

**答案:** netstat -s -p TCP 30

### 5.1.3 同步练习

1. 命令“ping 210.45.40.1 -t -l 512”的含义是什么?
2. 命令“tracert -h 10 -w 50 210.45.40.1”的含义是什么?
3. 为了分析一台安装了 Windows Server 2003 服务器的网络流量,使用查看网络状态信息工具 netstat。如果想每 30 秒显示一下 UDP 连接情况,并进行统计,该使用哪些参数(写出完整命令)?

4. 某台安装了 Windows Server 2003 服务器的装有多块网卡,不同网卡接入了不同网络,管理员通过 Windows Server 2003 中的 route 命令增加了路由表,那么我们使用什么命令来查看这个路由表呢?

5. 以下 Windows 命令中,可以用于验证端系统地址的是 (1); 可以用于识别分组传送路径的是 (2); 如果要终止一个 ping 会话,正确的操作是按 (3)。

- |                   |               |                 |                   |
|-------------------|---------------|-----------------|-------------------|
| (1) A. ping       | B. arp-a      | C. tracert      | D. telnet         |
| (2) A. ping       | B. traceroute | C. tracert      | D. routeprint     |
| (3) A. Ctrl+Break | B. Ctrl+C     | C. Ctrl+Alt+Del | D. Ctrl+Shift+Del |

### 5.1.4 同步练习参考答案

1. 连续向 IP 地址为 210.45.40.1 的主机发送大小为 512 字节的数据包,以检查该主机是否返回这些数据包的响应。

2. 查看数据包从本地主机到 IP 地址为 210.45.40.1 的主机所经过的路由,最大跃点数为 10,等待时间为 50ms。

3. netstat -s -p udp 30

4. netstat -r

5. (1) A      (2) C      (3) B

## 5.2 网络故障

### 5.2.1 考点辅导

#### 5.2.1.1 网络故障诊断与排除的基本概念

网络故障诊断是以网络原理、网络配置和网络运行的知识为基础,从故障现象出发,以网络诊断工具为手段获取诊断信息、确定网络故障点、查找问题的根源、排除故障、恢复网络正常运行的软件或者硬件。网络故障通常有以下几种可能:

- 物理层中物理设备相互连接失败或者硬件及线路本身的问题;
- 数据链路层网络设备的接口配置问题;
- 网络层网络协议配置或操作错误;
- 传输层设备性能或通信阻塞的问题;
- 上三层或网络应用程序错误。

网络故障的诊断过程应该沿着 OSI 七层模型从物理层开始向上进行。首先检查物理层,然后检查数据链路层,以此类推,设法确定通信失败的故障点,直到系统通信正常为止。

网络诊断可以使用包括局域网或广域网分析仪在内的多种工具:路由器诊断命令、网络管理工具和其他故障诊断工具。一般情况下查看路由表是开始解决网络故障时的首选。ICMP 的 ping、trace 命令和 Cisco 的 show 命令、debug 命令是获取故障诊断有用信息的网络工具。通常使用一个或多个命令收集相应的信息,在给定情况下,确定使用什么命令获取所需要的信息。

网络故障往往以某种症状表现出来,对每一个症状使用特定的故障诊断工具和方法都能查找出一个或多个故障原因。

#### 5.2.1.2 网络故障的分类

根据网络故障的性质把网络故障分为物理故障(硬件故障)与逻辑故障(软件故障),也可以根据网络故障的对象把网络故障分为线路故障、路由器故障和主机故障。

##### 1. 按网络故障的性质分类

首先介绍按照网络故障不同性质而划分的物理故障(硬件故障)与逻辑故障(软件故障)。

##### (1) 物理故障(硬件故障)

物理故障指的是设备或线路损坏、插头松动、线路受到严重电磁干扰等情况。

##### (2) 逻辑故障(软件故障)

逻辑故障中最常见的情况就是配置错误,就是指由于网络主机或网络设备的配置原因而导致的网络异常或故障。配置错误可能是主机、交换机或路由器端口参数设定有误,或路由器路由配置错误以至于路由循环或找不到远端地址,或者是路由掩码设置错误等。比如,同样是网络中的线路故障,该线路没有流量,但又可以 ping 通线路的两端端口,这时就很有可能是路由配置错误了。遇到这种情况,我们通常用“路由跟踪程序”(在不同系统



中的路由跟踪命令并不相同,在 Windows 环境下使用 `tracert` 命令,在 Linux 或 Unix 下使用 `traceroute` 命令,在 Cisco 路由器中使用 `trace` 命令),它和 `ping` 命令类似,最大的区别在于路由跟踪程序是把端到端的线路按线路所经过的路由器分成多段,然后以每段返回响应与延迟。如果发现在路由跟踪程序的结果中某一段之后,两个 IP 地址循环出现,这时,一般就是线路远端把端口路由又指向了线路的近端,导致 IP 数据包在该线路上来回反复传递。这时,只需更改远端路由器端口配置,就能恢复线路正常。

逻辑故障的另一类情况就是一些重要进程或端口关闭,以及系统的负载过高。比如也是线路中断,没有流量,用 `ping` 发现线路端口不通,检查发现该端口处于 `down` 的状态,这就说明该端口已经关闭,因此导致故障。这时只需重新启动该端口,就可以恢复线路的连通了。还有一种常见的故障情况是路由器的负载过高,表现为路由器 CPU 温度太高、CPU 利用率太高,以及内存剩余太少等,如果因此影响网络服务质量,最直接也是最好的办法就是更换路由器,当然要换个好点的。

## 2. 按网络故障发生地址分类

网络故障根据故障的不同对象也可以划分为线路故障、路由器故障和主机故障。

### (1) 线路故障

线路故障最常见的情况就是线路不通。诊断这种情况应首先检查该线路上流量是否还存在,然后用 `ping` 检查线路远端的路由器端口能否响应,用 `traceroute` 检查路由器配置是否正确,找出问题逐个解决。

### (2) 路由器故障

线路故障中很多情况都涉及到路由器,因此也可以把一些线路故障归结为路由器故障。检测路由器故障,需要利用 MIB 变量浏览器,用它收集路由器的路由表、端口流量数据、计费数据、路由器 CPU 的温度、负载以及路由器的内存剩余量等数据。通常情况下网络管理系统有专门的管理进程不断地检测路由器的关键数据,并及时给出报警。

### (3) 主机故障

主机故障常见的现象就是主机的配置不当。像主机配置的 IP 地址与其他主机冲突,或 IP 地址根本就不在子网范围内,由此导致主机无法连通。主机的另一常见故障就是安全故障。

## 5.2.1.3 网络故障的分层诊断技术

### 1. 物理层及其诊断

物理层是 OSI 分层结构体系中最基础的一层,它建立在通信媒体的基础上,实现系统和通信媒体的物理接口,为数据链路实体之间进行透明传输,为建立、保持和拆除计算机和网络之间的物理连接提供服务。物理层的故障主要表现在设备的物理连接方式不恰当;连接电缆不正确。确定路由器端口物理连接是否完好的最佳方法是使用 `show interface` 命令,检查每个端口的状态,解释屏幕输出信息,查看端口状态、协议建立状态和 EIA 状态。

### 2. 数据链路层及其诊断

数据链路层的主要任务是使网络层无须了解物理层的特征而获得可靠的传输。数据链路层为通过链路层的数据进行封装和拆封装、差错检测和一定程度的校正,并协调共享介

质。查找和排除数据链路层的故障，需要查看路由器的配置。

### 3. 网络层及其诊断

网络层提供建立、保持和释放网络层连接的手段，包括路由选择、流量控制、传输确认、中断、差错及故障恢复等。排除网络层故障的基本方法是沿着从源到目标的路径，查看路由器路由表，同时检查路由器接口的 IP 地址。如果路由没有在路由表中出现，应该通过检查来确定是否已经输入适当的静态路由、默认路由或者动态路由，然后手工配置一些丢失的路由，或者排除一些动态路由选择过程的故障。

#### 5.2.1.4 局域网常见故障的排除

虽然网络故障原因多种多样，但总的来讲不外乎就是硬件问题和软件问题，说得再确切一些，这些问题就是网络连接性故障、网络协议故障和网络配置故障。

##### 1. 网络连接性故障

网络连接性是故障发生后首先应当考虑的原因。连接性的问题通常涉及到网卡、跳线、信息插座、网线、Hub、交换机、Modem 等设备和通信介质。其中，任何一个设备的损坏，都会导致网络连接的中断。连接性通常可采用软件和硬件工具进行测试验证。例如，当某一台电脑不能浏览 Web 时，在网络管理员的脑子里产生的第一个想法就是网络连接性的问题。到底是不是呢？可以通过测试进行验证。看得到网上邻居吗？可以收发电子邮件吗？ping 得通网络内的其他电脑吗？只要其中一项回答为“是”，那就可以断定本机到 Hub 或交换机的连接性没有问题。当然，即使都回答“否”，也不就表明连接性肯定有问题，而是可能会有问题，因为如果电脑的网络协议的配置出现了问题也会导致上述现象的发生。另外，看一看网卡和 Hub 或交换机接口上的指示灯是否闪烁及闪烁是否正常也是个不错的主意。

排除了由于电脑网络协议配置不当而导致故障的可能后，就应该查看网卡和 Hub 的指示灯是否正常，测量网线是否畅通。

##### (1) 故障表现

连接性故障通常表现为以下几种情况：

- ① 电脑无法登录到服务器；
- ② 电脑无法通过局域网接入 Internet；
- ③ 电脑在【网上邻居】中只能看到自己，而看不到其他电脑，从而无法使用其他电脑上的共享资源和共享打印机；
- ④ 电脑无法在网络内实现访问其他电脑上的资源；
- ⑤ 网络中的部分电脑运行速度异常缓慢。

##### (2) 故障原因

以下原因可能导致连接性故障：

- ① 网卡未安装，或未安装正确，或与其他设备有冲突；
- ② 网卡硬件故障；
- ③ 网络协议未安装，或设置不正确；
- ④ 网线、跳线或信息插座故障；



⑤ Hub 或交换机电源未打开, Hub 或交换机硬件故障, Hub 或交换机端口硬件故障;

⑥ UPS 电源故障。

### (3) 故障排除方法

#### ① 确认连接性故障

当出现一种网络应用故障,如无法接入 Internet 时,首先尝试使用其他网络应用,如查找网络中的其他电脑,或使用局域网中的 Web 浏览等。如果其他网络应用可正常使用,如虽然无法接入 Internet,却能够在“网上邻居”中找到其他电脑,则可 ping 通其他电脑,即可排除连接性故障原因。如果其他网络应用均无法实现,则继续下面操作。

#### ② 看 LED 灯判断网卡的故障

首先查看网卡的指示灯是否正常。正常情况下,在不传送数据时,网卡的指示灯闪烁较慢,传送数据时,闪烁较快。如果是不亮,或者是长亮不灭,都表明有故障存在。如果网卡的指示灯不正常,需关掉电脑更换网卡。对于 Hub 或交换机的指示灯,凡是插有网线的端口,指示灯都亮。Hub 指示灯的作用只能指示该端口是否连接有终端设备,而不能显示通信状态。有的交换机指示灯则通过不同的颜色来表示不同的通信状态,例如用绿色表示正常通信,用橙色表示阻断通信。

#### ③ 用 ping 命令排除网卡故障

使用 ping 命令, ping 本地的 IP 地址或主机名(如 server01),检查网卡和 IP 网络协议是否安装完好。如果能 ping 通,说明该电脑的网卡和网络协议设置都没有问题,问题出在电脑与网络的连接上。因此,应当检查网线和 Hub(或交换机)及 Hub(或交换机)的接口状态,如果无法 ping 通,只能说明 TCP/IP 协议有问题。这时可以在电脑的【控制面板】的【系统】中,查看网卡是否已经安装或是否出错。如果在系统中的硬件列表中没有发现网络适配器,或网络适配器前方有一个黄色的“!”,说明网卡未安装正确,需将未知设备或带有黄色“!”的网络适配器删除。刷新后,重新安装网卡,并为该网卡正确安装和配置网络协议,然后进行应用测试。如果网卡无法正确安装,说明网卡可能损坏,必须换一块网卡重试。如果网卡安装正确,则故障原因是协议未安装。

④ 如果确定在网卡和协议都正确的情况下,网络还是不通,可以初步断定是 Hub(或交换机)和双绞线的问题。为了进一步进行确认,可再换一台主机用同样的方法进行判断。如果其他电脑与本机连接正常,则故障一定在先前那台主机和 Hub(或交换机)的接口上。

⑤ 如果确定 Hub(或交换机)有故障,应首先检查 Hub(或交换机)的指示灯是否正常,如果先前那台电脑与 Hub(或交换机)连接的接口灯不亮,说明该 Hub(或交换机)的接口有故障。

⑥ 如果 Hub(或交换机)没有问题,则检查电脑到 Hub 的那一段双绞线和所安装的网卡是否有故障。判断双绞线是否有问题可以通过双绞线测试仪或用两块三用表分别由两个人在双绞线的两端测试。主要测试双绞线的 1、2 和 3、6 四条线(其中 1、2 线用于发送,3、6 线用于接收)。如果发现有一根不通就要重新制作。

通过上面的操作,我们就可以判断故障是否出在网卡、双绞线或 Hub(或交换机)上,从而一一予以排除。

## 2. 网络协议故障

没有网络协议,网络设备和电脑之间就无法实现通信,不能实现资源共享。

### (1) 协议故障的表现

协议故障通常表现为以下几种情况:

- ① 电脑无法登录到服务器。
- ② 电脑在【网上邻居】中既看不到自己,也无法在网络中访问其他电脑。
- ③ 电脑在【网上邻居】中能看到自己和其他成员,但无法访问其他电脑。
- ④ 电脑无法通过局域网接入 Internet。

### (2) 故障原因分析

- ① 协议未安装:实现局域网通信,需安装 NetBEUI 协议,这有助于提高网络速度。
- ② 协议配置不正确:TCP/IP 协议涉及到的基本参数有四个,包括 IP 地址、子网掩码、DNS、网关,任何一个设置错误,都会导致故障发生。

### (3) 排除步骤

当电脑出现以上协议故障现象时,应当按照以下步骤进行故障的定位:

- ① 检查电脑是否安装 TCP/IP 和 NetBEUI 协议,如果没有,建议安装这两个协议,并把 TCP/IP 参数配置好,然后重新启动电脑;
- ② 使用 ping 命令,测试与其他电脑的连接情况;
- ③ 在【控制面板】的【网络】属性中,单击【文件及打印共享】按钮,在弹出的【文件及打印共享】对话框中检查一下,看看是否选中了【允许其他用户访问我的文件】和【允许其他电脑使用我的打印机】复选框,或者选中了其中的一个。如果都没有选中,则应全部选中或选中其中一个,否则将无法使用共享文件夹;
- ④ 系统重新启动后,双击【网上邻居】,将显示网络中的其他电脑和共享资源。如果仍看不到其他电脑,可以使用【查找】命令,能找到其他电脑,就可以;
- ⑤ 在【网络】属性的【标识】中重新为该电脑命名,使其在网络中具有惟一性。

## 3. 网络配置故障

配置错误也是导致故障发生的重要原因之一。服务器、工作站、交换机、路由器都有自己的配置选项,如果网络管理员对服务器、交换机、路由器等有不当设置就会导致网络故障,例如对服务器权限的设置不当,会导致资源无法共享的故障。电脑的使用者对电脑设置的修改,也往往会产生一些令人意想不到的访问错误,例如网卡配置不当,会导致无法连接的故障。

### (1) 故障表现及分析

配置故障更多地表现在不能实现网络所提供的各种服务上,如不能访问某一台电脑等。因此,在修改配置前,必须做好原有配置的记录,并且最好进行备份。

配置故障通常表现为以下两种:

- ① 电脑只能与某些电脑而不是全部电脑进行通信;
- ② 电脑无法访问任何其他设备。

### (2) 配置故障排除步骤

首先检查发生故障电脑的相关配置。如果发现错误,修改后,再测试相应的网络服务



能否实现。如果没有发现错误,或相应的网络服务不能实现,可执行下述步骤。

测试系统内的其他电脑是否有类似的故障,如果有同样的故障,说明问题出在网络设备上,如 Hub 或交换机。反之,检查被访问电脑对该电脑所提供的服务。

网络故障虽然多种多样,但并非无规律可循。随着理论知识和经验技术的积累,故障排除将变得越来越快、越来越简单。严格的网络管理,是减少网络故障的重要手段;完善的技术档案,是排除故障的重要参考;有效的测试和监控工具则是预防、排除故障的有力助手。

## 5.2.2 典型例题分析

**例 1** 某公司内部有一个采用 TCP/IP 作为传输协议的 100Base-TX 局域网,包括 1 台服务器和 20 台客户机,通过一台 16 端口的交换机与一台 8 端口共享集线器级联,其网络结构如图 5.1 所示。服务器上运行 DHCP 服务软件,客户机的 IP 地址由 DHCP 服务程序自动分配。主机 B 登录网络后在网络邻居中只能看到自己的主机名,而看不到服务器和其他客户机的主机名,列出可能出现的硬件和软件故障。(2004 年下半年网络管理员下午试题二【问题 3】)

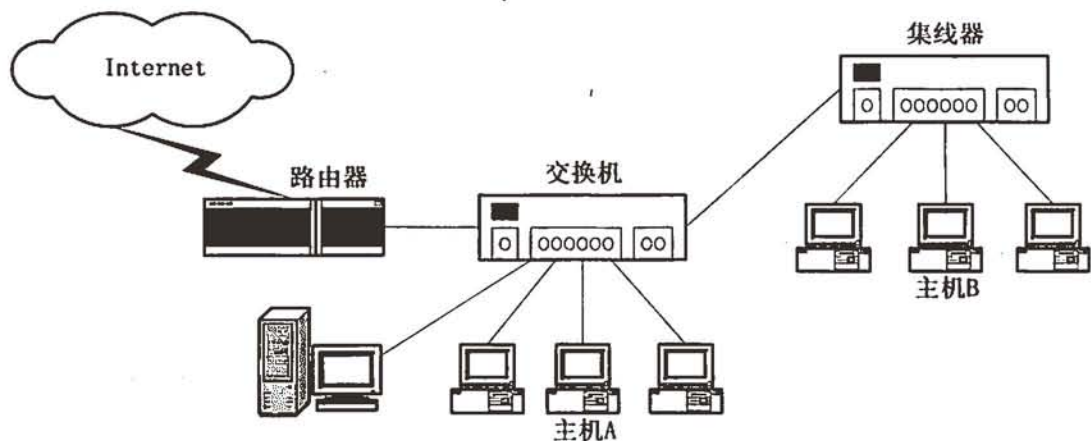


图 5.1 某公司网络拓扑图

**分析:** 该题主要考查考生对网络故障排除的掌握情况。

电脑在【网上邻居】中只能看到自己,而看不到其他电脑,引起这种故障的原因有很多,既可能是硬件故障,也可能是软件故障。对于硬件故障来说,可能有客户机的网卡坏了;网线、跳线或信息插座故障;Hub 电源未打开、Hub 硬件故障或 Hub 端口硬件故障。对于软件故障来说,可能是网卡驱动程序未安装,或安装不正确,或与其他设备有冲突;网络协议未安装或设置不正确(TCP/IP 协议没有安装,IP 地址和子网掩码设置不正确);DHCP 服务器设置错误或 IP 地址资源不足,客户机无法租约到 IP 地址。

**答案:** 硬件故障主要有:网卡故障、通信介质故障(包括网线、跳线或信息插座故障)、Hub 硬件故障(包括 Hub 电源未打开、Hub 硬件故障或 Hub 端口硬件故障),软件故障包括:网卡驱动程序未安装或安装不正确,网络协议未安装或设置不正确, DHCP 服务器设置错误或 IP 地址资源不足。

**例 2** 有一小型局域网, 服务器为 Windows NT 操作系统, 各工作站为 Windows 98 操作系统。以前局域网一直工作正常, 后来有一台工作站重新安装 Windows 98 之后, 这台电脑通过网上邻居浏览其他电脑的速度非常慢, 而且只能看到一部分电脑, 有的电脑却看不到, 而其他电脑相互之间一切正常。检查 IP 地址与子网掩码没有错误, 域名与工作组也相同。列出可能出现该问题的原因。

**分析:** 该题主要考查考生对网络故障排除的掌握情况。

通过以上描述, 我们可以得出以下结论: 第一, 既然能看到一部分电脑, 说明网络连接正常, 而且正确安装了网卡驱动程序和网络通讯协议; 第二, 既然 IP 地址与子网掩码没有错误, 说明 IP 地址信息设置正确; 第三, 既然域名与工作组相同, 应当能够非常快地找到同一工作组内的其他用户才对。

然而, 事实上, 不仅计算机之间的连接速度非常慢, 而且只能找到其中的一部分计算机, 这才是问题的关键。故障的原因和解决方法如下:

第一, 没有安装 NetBEUI 协议。TCP/IP 是一个效率不高的协议, 因此, 在小型局域网中, 通常都使用占用系统资源更少、而且效率更高的 NetBEUI 协议。另外, 只安装有 TCP/IP 协议的 Windows 98 计算机要想加入到 Windows NT 域, 也必须安装 NetBEUI 协议。第二, 网卡驱动程序有缺陷。虽然许多网卡都采用相同的芯片组, 但是, 驱动程序并不完全相同。尽管有缺陷的驱动程序并不一定会导致通信失败, 但却往往会在传输效率上大打折扣。因此, 应当确认网卡驱动程序的选择和安装无误。第三, 由于 Windows NT 没有活动目录(Active Directory)功能, 无法快速有效地组织网络资源。因此, 未被访问过的计算机就可能不会出现在网上邻居中。试着在服务器上使用“查找”功能, 利用计算机名称或 IP 地址查找一下无法显示在网上邻居中的计算机。通常情况下, 查找到的计算机就会自动显示在网上邻居中。

**答案:** 没有安装 NetBEUI 协议、网卡驱动程序有问题、Windows NT 没有活动目录功能。

**例 3** 有两台同属财务部的笔记本电脑 A 和 B。两台计算机都配置了 TCP/IP 和 NetBEUI 协议, A 抱怨当他连接网络时, 能够使用 NetBEUI 协议与 B 通信, 但是不能使用 TCP/IP 通信, 他也不能与网络上使用 TCP/IP 的其他计算机进行通信, B 告诉他一个星期以前自己也遇到同样的事情, 尽管现在他可以与使用 TCP/IP 的其他计算机进行通信。请问最有可引起问题的原因是什么? 为什么?

**分析:** 该题主要考查考生对网络故障排除的掌握情况。

由于这两台电脑能够通过 NetBEUI 协议互相通信, 这就说明这两台电脑和网络的硬件上没有故障, 否则他们就不能通过 NetBEUI 协议互相通信了, 因此故障是出在软件上。我们知道, 在一个局域网中要使用 TCP/IP 协议进行通信时, 计算机必须有一个合适的 IP 地址, 而且这个地址在整个网络中是惟一的。若两台计算机的 IP 地址相同, 则后启动的计算机的 TCP/IP 协议将被禁用, 这样就无法与使用 TCP/IP 的其他计算机进行通信。由于 B 在一个星期以前也遇到同样的故障, 因此该故障最有可能是 A 和 B 的计算机有相同的 IP 地址。

**答案:** A 和 B 的计算机有相同的 IP 地址。原因略。

### 5.2.3 同步练习

1. 有一台 PC 机无法访问其他计算机和 Internet, 网络设置都正确, 但网卡和 Hub 上的指示灯都不亮。请列出可能出现的故障原因。

2. 有一台 PC 机无法访问其他计算机和 Internet, 通过 ping 命令 Ping 127.0.0.1 成功, ping 自己的网卡地址却不成功。请列出可能出现的故障原因。

3. 有一台客户机, 能够通过网上邻居看到其他客户机和服务器, 但就无法访问到 Internet(通过 IP 地址也不行), 但其他客户机却可以, 请问最有可能的原因是什么?

4. 某公司的域名为 abc.com.cn, 内部有一个名字为 www.abc.com.cn 的 Web 服务器, 有一台客户机在浏览地址栏中输入 www.abc.com.cn 却无法访问内部的 Web 服务器, 输入 Web 服务器的 IP 地址却可以访问, 但其他客户机却可以。请问最有可能的原因是什么?

5. 网络配置如下: 两个子网, 一个路由器。路由器有两个接口: 网络 A 为 167.191.32.1, 网络 B 为 167.191.64.1, 所有计算机使用一个子网掩码 255.255.224.0。你的 Windows 2000 工作站连接不到网络 A 上的远程服务器, 但网络 B 上所有其他工作站都能连接上。你的工作站位于网络 B。当在工作站上运行 ipconfig/all 命令时, 接收到如下输出:

IP 地址是: 167.191.82.17; 子网掩码是 255.255.224.0; 默认网关是 167.191.32.1。导致这一问题的最可能原因是什么?

### 5.2.4 同步练习参考答案

1. 网卡坏了、网线、跳线或信息插座故障、Hub 电源未打开、Hub 硬件故障或 Hub 端口硬件故障。

2. 网卡坏了、IP 地址与其他主机冲突。

3. 默认网关没有设置或设置不正确。

4. TCP/IP 属性的 DNS 服务器设置错误或没设置。

5. 错误的默认网关, 默认网关应当为 167.191.64.1。

## 5.3 数据备份与恢复

### 5.3.1 考点辅导

#### 5.3.1.1 数据备份与恢复的概述

数据备份是用来防止由于硬件或媒体失效或者其他损坏事件的故障而丢失数据。如果系统中的数据丢失, 则通过备份实用程序就可以方便地从存档的副本中恢复数据, 同时能将系统从各种故障中恢复正常运行。

1. 导致数据失效的原因

(1) 计算机软硬件故障

由计算机软硬件故障而引起数据失效是发生概率最大的一类故障。这类故障主要包括机器损坏、磁盘故障、突然停电、病毒感染而破坏数据等。预防方法主要有采用本地双机热备份,实现系统冗余,增强业务系统的高可用性。

(2) 人为操作故障

另一类主要故障由人为操作失误而引起数据失效,对管理较严、人员素质较高的单位,会偶尔发生,但对管理较松、人员培训不足的单位,会经常发生。

预防方法主要是提高系统自动化运行管理水平,做好本地数据冷备份,减少人为操作与干预,或制定严格的管理规范,避免误操作。

(3) 生产地点的灾难

由于生产地点的灾难而导致数据的失效尽管发生概率较小,但毕竟有偶然发生的可能性,这类灾难包括火灾、水灾,地震甚至战争。预防方法主要是灾难恢复中心。

2. 备份系统的目标

理想的备份系统应该是全方位、多层次的。首先,要使用硬件备份来防止硬件故障;如果由于软件故障或人为误操作造成了数据的逻辑损坏,则使用网络存储备份系统和硬件容错相结合的方式。这种结合方式构成了对系统的多级防护,不仅能够有效地防止物理损坏,还能够彻底防止逻辑损坏。

在网络系统安全建设中必不可少的一个环节就是数据的常规备份和历史保存。一般在生产本地的备份目的主要有两个:一是生产系统的业务数据由于系统或人为误操作造成损坏或丢失后,可及时在生产本地实现数据的恢复;二是在发生地域性灾难(地震、火灾、机器毁坏等)时,可及时在本地或异地实现数据及整个系统的灾难恢复。

考虑到生产本地环境安全性原因,常规数据备份一般要求一份数据至少应有两个拷贝,一份放在生产中心以保证数据的正常恢复和数据查询恢复,另一份则要移到异地保存,以保证在生产本地出现灾难后最低限度的数据恢复。此外,更应建立历史归档数据的异地存放制度,从而确保对历史业务数据的可靠恢复与有效稽核的实现。

3. 备份策略

备份策略描述了每天的备份以什么方式、使用什么备份介质进行,是系统备份方案的具体实施细则。在备份策略制定完毕后,应严格按照制度进行日常备份,否则将无法达到备份策略的目标。

(1) 数据备份方式

数据备份有多种方式:正常备份、复制备份、差异备份、增量备份、定期备份等,如表 5.1 所示。

表 5.1 备份方式

类型	备份内容	是否消除备份标记
正常备份	选择文件和文件夹	是
复制备份	选择文件和文件夹	否
差异备份	选择自从上次备份后改变的文件和文件夹	否
增量备份	选择自从上次备份后改变的文件和文件夹	是



类型	备份内容	是否消除备份标记
定期备份	选择每天改变的文件和文件夹	否

### ① 正常备份

正常备份是将选定的文件都备份下来,并把每一个文件都标记为已经备份(换句话说,就是要设置档案文件的位)。对于正常备份,只需要最新的备份文件或磁带的副本,就能还原所有的文件。在通常情况下,在首次创建备份设置时应进行正常备份。

### ② 复制备份

复制备份是备份选定的所有文件,但不对正在被备份的每一个文件都做标记(换句话说,就是不设置档案文件的位)。如果希望在正常备份和增量备份之间备份文件,复制备份是非常有效的,因为复制备份操作不影响其他备份操作。

### ③ 差异备份

差异备份是备份自从最后一次正常备份或增量备份以来创建或经过修改的文件。同样,差异备份后也不将文件标记为已经做过备份(换句话说,就是不设置档案文件的位)。如果正在进行按正常备份和差异备份的联合备份,那么还原增量备份文件和文件夹时,则要求用户已经进行最后一次正常备份及最后一次差异备份。

### ④ 增量备份

增量备份是只备份自从最后一次正常备份或增量备份以来又创建或修改过的文件。增量备份将文件标记为已经做过备份(换句话说,就是要设置档案文件的位)。如果使用了正常备份和增量备份的联合备份,将需要进行最后的正常备份集及所有的增量备份集,以便还原数据。

### ⑤ 定期备份

定期备份是把选定的已经修改的所有文件按事先安排的日期进行定期复制。备份的文件也不必标记为已经被备份(换句话说,就是不设置档案文件的位)。

## (2) 数据备份策略举例(如表 5.2 所示)

表 5.2 数据备份策略举例

方案	星期一	星期二	星期三	星期四	星期五
方案 1	正常备份	差异备份	差异备份	差异备份	差异备份
方案 2	正常备份	增量备份	增量备份	增量备份	增量备份
方案 3	正常备份	差异备份	差异备份	差异备份	差异备份
			复制备份		

方案 1: 该方案使用正常备份和差异备份联合方法备份数据,其缺点是比较消耗时间,在数据变化非常频繁时尤为明显。但是这种方法还原数据时非常容易,因为备份集通常只存放在少数几种磁盘或磁带上。

方案 2: 该方案使用正常备份和增量备份联合方法备份数据,所要求的存储空间最小,是速度最快的备份方法。但是,这种联合方法还原文件消耗时间长,而且还原困难,因为备份集可以存放在几个磁盘或磁带上。

方案 3: 该方案也使用正常备份和差异备份联合方法备份数据, 但在星期三增加一次复制备份, 以提高系统的可靠性。

#### 4. 数据恢复策略

数据恢复策略在整个备份制度中占有相当重要的地位。因为它关系到系统在经历灾难后能否迅速恢复。数据恢复操作通常可以分为三类。第一类是全盘恢复, 第二类是个别文件恢复, 还有一种值得一提的是重定向恢复。

##### (1) 全盘恢复

全盘恢复一般应用在服务器发生意外灾难导致数据全部丢失、系统崩溃或是有计划的系统升级、系统重组等, 也称为系统恢复。

##### (2) 个别文件恢复

由于操作人员的水平不同, 因此个别文件恢复可能要比全盘恢复常见得多, 利用网络备份系统的恢复功能, 我们很容易恢复受损的个别文件。只需浏览备份数据库或目录, 找到该文件, 启动恢复功能, 软件将自动驱动存储设备, 加载相应的存储媒体, 然后恢复指定文件。

##### (3) 重定向恢复

重定向恢复是将备份的文件恢复到另一个不同的位置或系统上去, 而不是进行备份操作时它们当时所在的位置。重定向恢复可以是整个系统恢复也可以是个别文件恢复。重定向恢复时需要慎重考虑, 要确保系统或文件恢复后的可用性。

为了防备数据丢失, 我们需要做好详细的灾难恢复计划, 同时还要定期进行灾难演练。每过一段时间, 应进行一次灾难演习。可以利用淘汰的机器或多余的硬盘进行灾难模拟, 以熟练灾难恢复的操作过程, 并检验所生成的灾难恢复软盘和灾难恢复备份是否可靠。

### 5.3.1.2 Windows Server 2003 的数据备份与恢复

#### 1. 备份整个系统

在备份系统文件时, 可以在备份向导的提示下进行, 也可以直接对选中的文件进行备份。下面是备份整个系统的具体操作步骤。

(1) 打开【开始】菜单, 选择【附件】|【系统工具】|【备份】命令, 打开【备份或还原向导】对话框, 如图 5.2 所示。

(2) 在【备份或还原向导】对话框中若消除【总是以向导模式启动】选项, 则下次启动时将不出现该对话框。点击【高级模式】超链接, 打开【备份工具】对话框, 如图 5.3 所示。

(3) 在【备份工具】对话框中, 单击【备份向导】按钮, 进入【备份向导】的【欢迎使用备份向导】界面, 如图 5.4 所示。

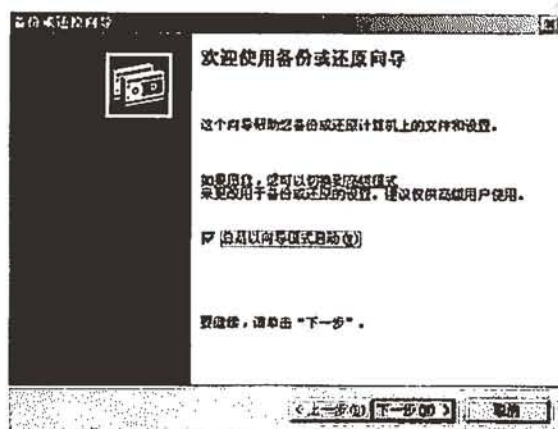


图 5.2 【备份或还原向导】对话框

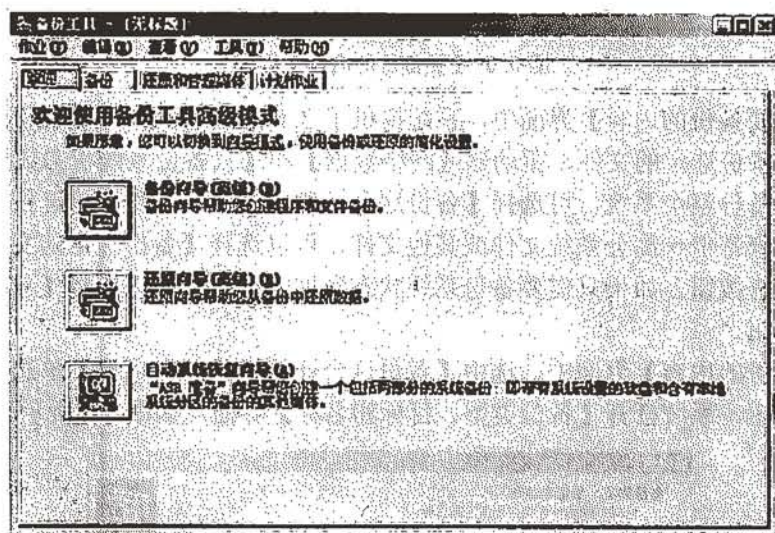


图 5.3 【备份工具】对话框

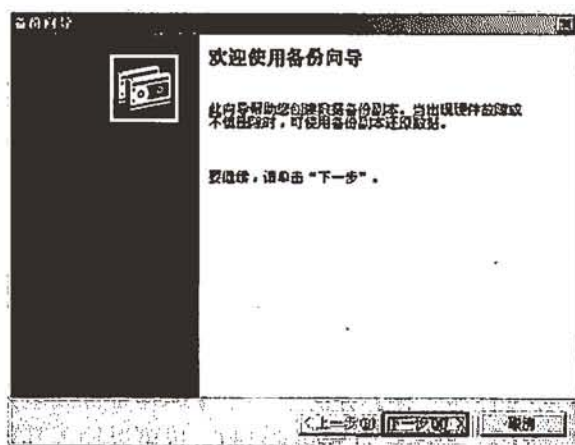


图 5.4 【备份向导】对话框

(4) 单击【下一步】按钮，打开【要备份的内容】界面，如图 5.5 所示。

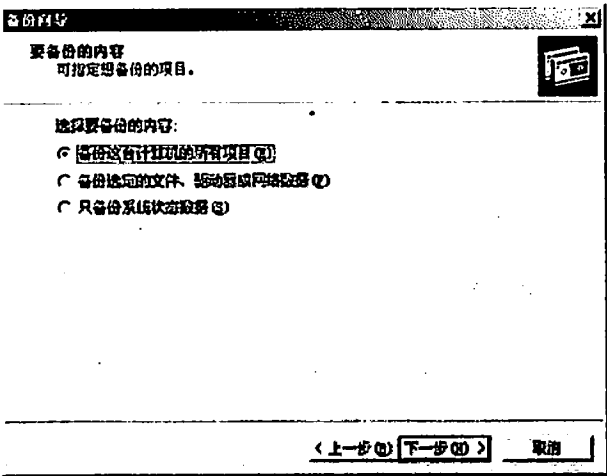


图 5.5 【要备份的内容】界面

(5) 在【要备份的内容】界面中，系统提供了 3 种备份方式，即【备份这台计算机的所有项目】、【备份选定的文件、驱动器或网络数据】和【只备份系统状态数据】。

如果需要备份整个系统，可选择【备份这台计算机的所有项目】单选按钮。如果需要通过自己选择来备份一部分系统文件或其他文件，可以选择【备份选定的文件、驱动器或网络数据】单选按钮。如果只需要备份系统状态数据的文件，可以选择【只备份系统状态数据】单选按钮。

在【要备份的内容】界面中，选中【备份这台计算机的所有项目】单选框，然后单击【下一步】按钮，系统打开【备份类型、目标和名称】界面，如图 5.6 所示。

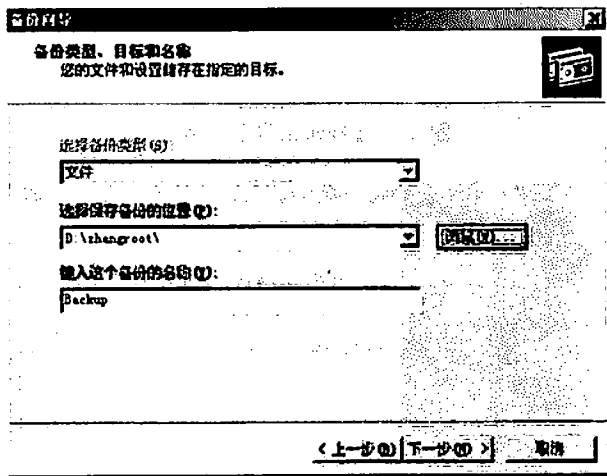


图 5.6 【备份类型、目标和名称】界面

(6) 在【备份类型、目标和名称】界面中，在【选择备份类型】下拉列表框中，系统默认备份媒体类型为【文件】，文件名为 Backup.bkf，也可以输入其他类型和文件名取代默认值。



可以单击【浏览】按钮,打开【打开文件】对话框,在磁盘上选择保存备份的位置,然后再返回到【备份类型、目标和名称】界面。完成上述选择后单击【下一步】按钮,系统打开【完成备份向导】界面,如图 5.7 所示。

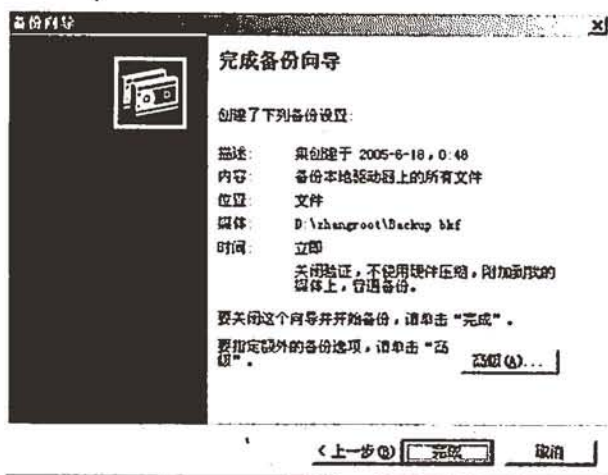


图 5.7 【完成备份向导】界面

(7) 在【完成备份向导】界面中,系统提示了系统备份的一系列信息,包括创建时间、创建的内容、媒体类型、备份方式等内容。如果需要指定更多的备份选项,可以单击【高级】按钮,打开【备份类型】界面,如图 5.8 所示。

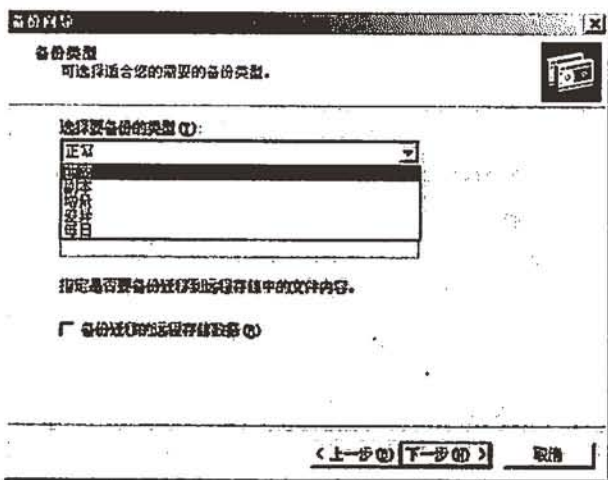


图 5.8 【备份类型】界面

(8) 在【备份类型】界面中,可以按需要运行不同类型的备份。在【选择要备份的类型】下拉列表框中可以选择不同的备份类型。其中包括【正常】、【副本】、【增量】、【差异】和【每日】5种备份类型。

(9) 如果选中【备份迁移的远程存储数据】复选框,则在备份的同时可以将系统文件保存到远程计算机上。完成上述设置后,单击【下一步】按钮,打开【如何备份】界面,如图 5.9 所示。



(12) 完成上述设置后,单击【下一步】按钮,打开【备份时间】界面,在【备份时间】界面中,可以指定运行备份的时间,既可以现在运行,也可以计划以后再运行。选择【现在】单选按钮可立即运行备份,如图 5.11 所示。

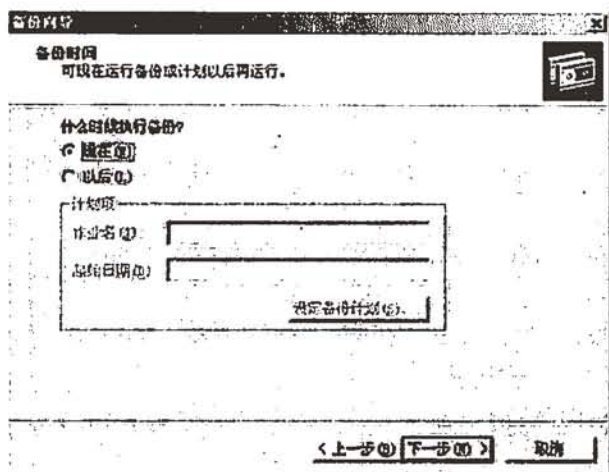


图 5.11 【备份时间】界面

(13) 如果选择【以后】单选按钮,可以计划以后运行备份,在【计划项】选项区域中的【作业名】文本框中输入作业的名称,同时系统默认起始日期为当前日期。单击【设定备份计划】按钮,打开【计划作业】对话框,同时系统默认打开【日程安排】选项卡,如图 5.12 所示。

(14) 在【日程安排】选项卡中可以设置计划任务的类型,包括【每天】、【每周】、【每月】、【一次性】、【在系统启动时】、【在登录时】和【在空闲时】等 7 种类型。在【开始时间】微调框中可以设定计划任务的开始时间。单击【高级】按钮可以继续设置一些高级选项。

选中【显示多项计划】复选框,可以在该对话框中同时显示多项计划,这时在对话框上部出现一个下拉列表框,从中可以新建或查看多项计划。

(15) 在【计划作业】对话框中,单击【设置】标签打开【设置】选项卡。在【设置】选项卡中,对于已经完成的计划任务可以选中【如果不计划再重新运行任务,请删除该任务】或【如超出 xx 小时 xx 分钟后,停止任务】复选框。在【空闲时间】选项区域中,可以设置【仅当计算机空闲时间超过 xx 分钟后,启动计划的任务】、【如果计算机还没有空闲很久,在 xx 分钟后重试】或【如果计算机在使用中,停止任务】。在【电源管理】选项区域中可以设置【如果计算机使用电池来运行,不要启动任务】、【如果启动电池模式,停止任务】或【唤醒这台计算机,运行此任务】,如图 5.13 所示。

(16) 上述设置完成后,单击【确定】按钮系统返回到【备份时间】对话框。在【备份时间】界面中,单击【下一步】按钮,打开【完成备份向导】对话框,如图 5.14 所示。

在【完成备份向导】界面中,其中的各选项与如前图 5.7 所示的【完成备份向导】界面中的选项基本相同,此处不再赘述。单击【完成】按钮,开始进行备份,备份完成后系统将返回到如前图 5.3 所示的【备份工具】对话框。

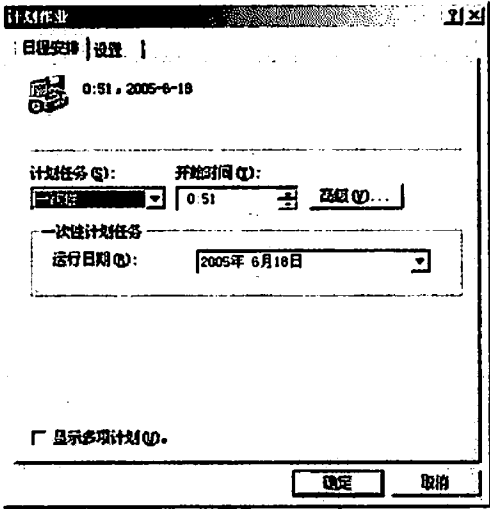


图 5.12 【日程安排】选项卡

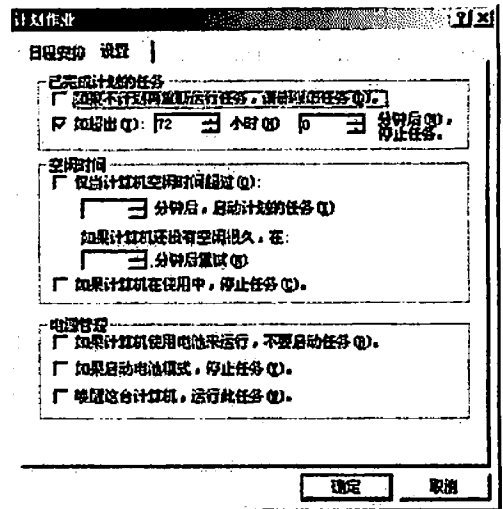


图 5.13 【设置】选项卡

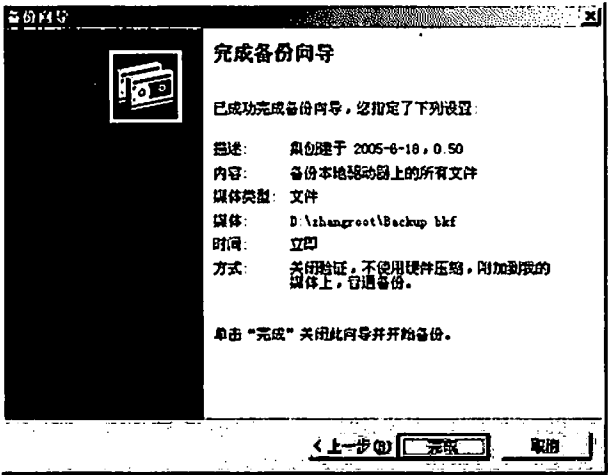


图 5.14 【完成备份向导】界面

2. 备份选定的内容

(1) 在如前图 5.5 所示的【要备份的内容】对话框中, 选中【备份选定的文件、驱动器或网络数据】单选按钮, 可以按照选定的文件、驱动器或网络数据进行备份, 如图 5.15 所示。

(2) 单击【下一步】按钮, 打开【要备份的项目】界面。如图 5.16 所示。

(3) 在【要备份的项目】界面中的【要备份的项目】列表框中, 左侧的目录区显示要备份的项目所在的目录, 可以从中选择某个目录。然后在右侧的文件显示区选择要备份的具体项目文件名。只需选中所需项目前面的复选框, 即可选中相应的驱动器、文件夹或文件。完成上述选择后, 单击【下一步】按钮, 打开如前图 5.6 所示的【备份类型、目标和名称】界面, 后面的操作步骤如前所述。



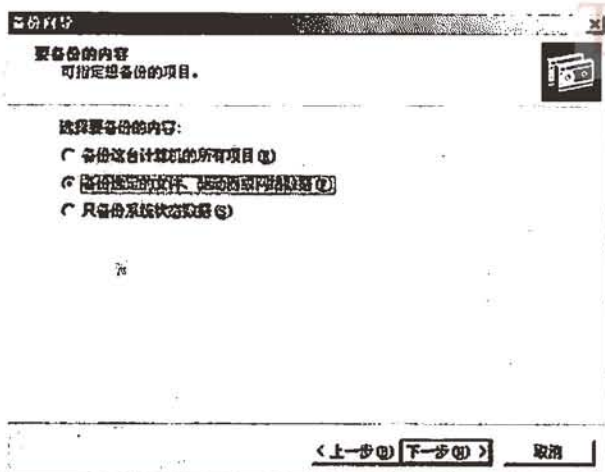


图 5.15 【要备份的内容】界面

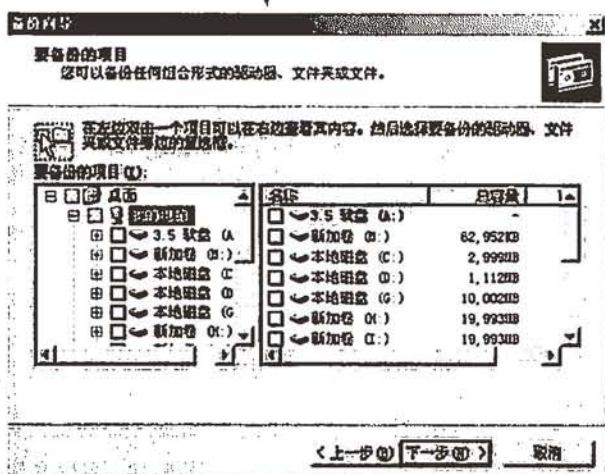


图 5.16 【要备份的项目】界面

### 3. 备份系统状态数据

(1) 在如前图 5.5 所示的【要备份的内容】界面中, 选择【只备份系统状态数据】单选按钮, 则可只备份系统文件, 如图 5.17 所示。

(2) 单击【下一步】按钮, 打开如前图 5.6 所示的【备份类型、目标和名称】界面。在该对话框的【键入这个备份的名称】文本框中输入要备份的媒体名或文件名(Backup.bkf)。也可以单击【浏览】按钮, 在打开的【打开文件】界面中选择保存文件的位置, 然后单击【打开】按钮返回到上一级对话框, 单击【下一步】按钮打开【完成备份向导】界面, 然后单击【完成】按钮打开【备份进度】对话框, 如图 5.18 所示。

(3) 在【备份进度】对话框中, 系统显示备份的进程及各项参数的当前设置状态, 包括【驱动器】、【标签】、【状态】、【进度】及已用时间和估计剩余时间、【正在处理】的文件名、【已经处理】的【文件数】和【字节数】等。完成备份后单击【报告】按钮打开备份文件的记录报表, 如图 5.19 所示。

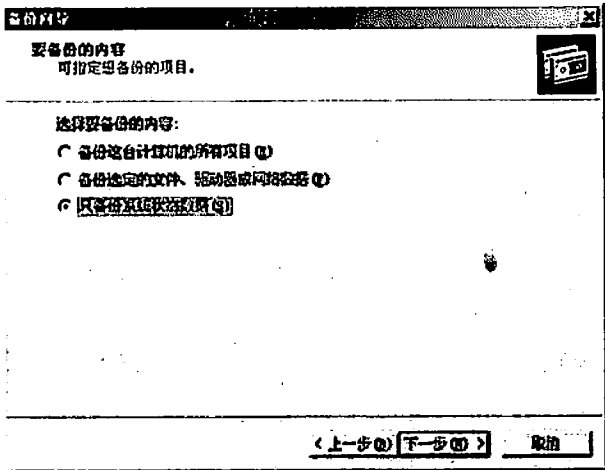


图 5.17 【要备份的内容】界面

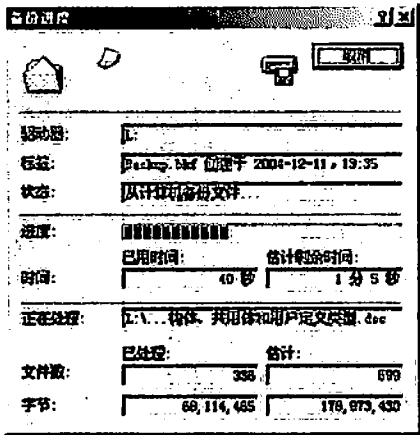


图 5.18 【备份进度】对话框

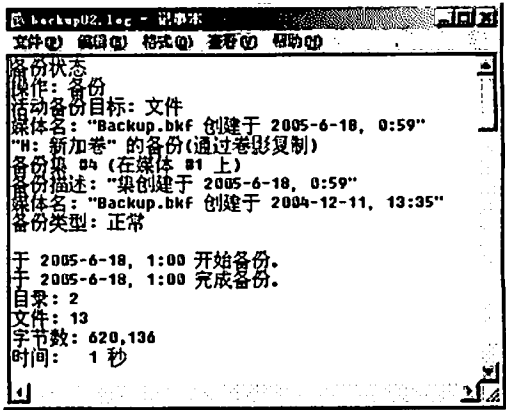


图 5.19 备份文件的记录报表

(4) 在【备份进度】对话框中单击【关闭】按钮即完成备份，此时系统生成一个名为 Backup.bkf 的备份文件，同时返回到如前图 5.3 所示的【备份工具】对话框。

注意：只能在本地计算机备份“系统状态”数据。即使是远程计算机上的管理员，也不能备份远程计算机上的“系统状态”数据。

5.3.1.3 Windows Server 2003 的数据恢复

通过系统文件或其他重要文件的备份，一旦系统发生故障或出现其他意外情况系统不能运行时，可以利用备份的数据文件迅速还原。这样可以确保系统的安全性和稳定性。

1. 利用还原向导还原备份

当出现硬件故障、意外删除或其他数据丢失或损坏时，利用还原向导可以还原以前备份的数据。

下面介绍数据还原的具体操作步骤。

(1) 在如前图 5.3 所示的【备份工具】对话框中单击【还原向导】按钮，打开【还原向导】对话框的【欢迎使用还原向导】界面，如图 5.20 所示。

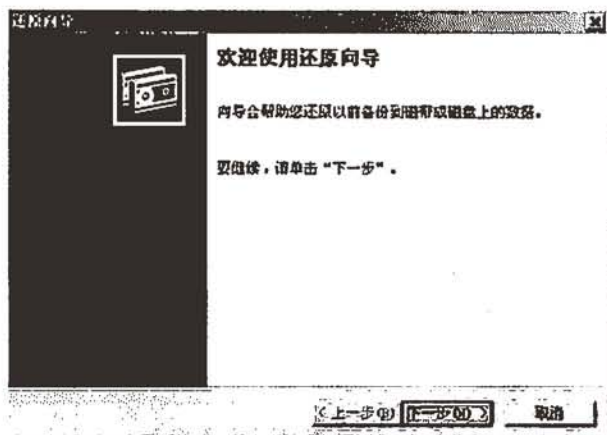


图 5.20 【欢迎使用还原向导】界面

(2) 在【欢迎使用还原向导】界面中，系统提示可以利用该向导帮助还原以前备份到磁盘或磁带上的数据。单击【下一步】按钮，打开【还原项目】界面。在该界面中，各选项与前图 5.15 所示的【要备份的项目】界面中的相应选项的含义基本相同，在此不再赘述，如图 5.21 所示。

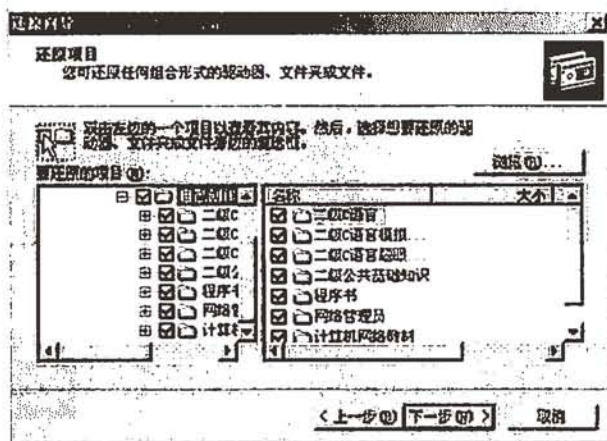


图 5.21 【还原项目】界面

(3) 设置好各项选项后，单击【下一步】按钮，打开【完成还原向导】界面，如图 5.22 所示。

(4) 在【完成还原向导】界面中，列出了还原选项的各项设置。如果需要指定额外的选项，可以单击【高级】按钮，打开【还原位置】界面。在该界面中可以指定还原的位置，包括【原位置】、【备用位置】和【单个文件夹】3 种选择。如果选择【备用位置】或【单个文件夹】，则提示指定【备用位置】，如图 5.23 所示。

(5) 当设置好还原的位置后，单击【下一步】按钮，系统将打开【如何还原】界面。在该界面中，可以选择还原已经在磁盘上的文件的方法，包括【保留现有文件】、【如果现

有文件比备份文件旧，将其替换】和【替换现有文件】3种方法，如图 5.24 所示。

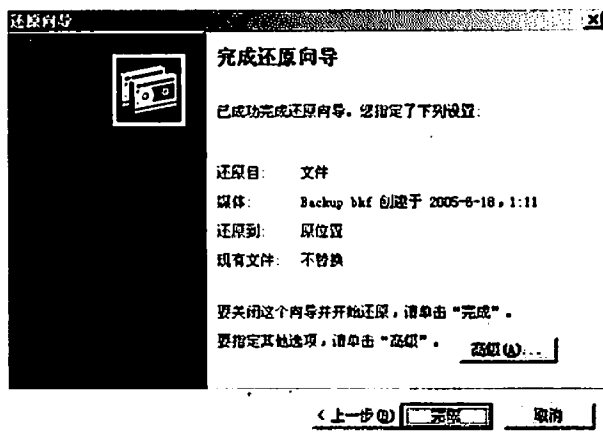


图 5.22 【完成还原向导】界面

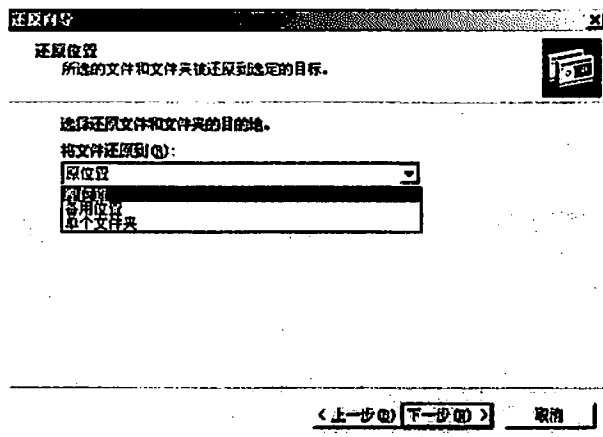


图 5.23 【还原位置】界面

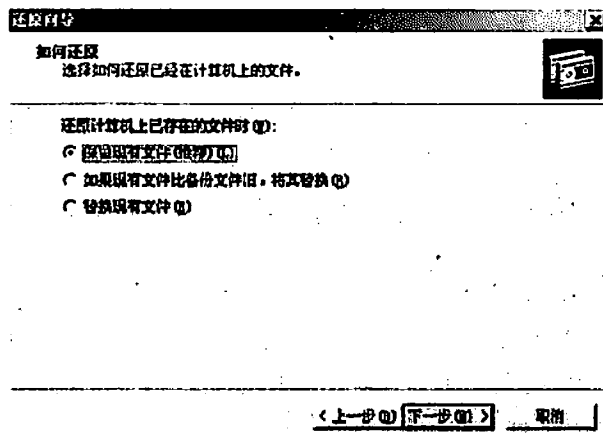


图 5.24 【如何还原】界面



(6) 单击【下一步】按钮，打开【高级还原选项】界面。在该对话框中可以选择还原安全措施或特殊系统文件，如图 5.25 所示。

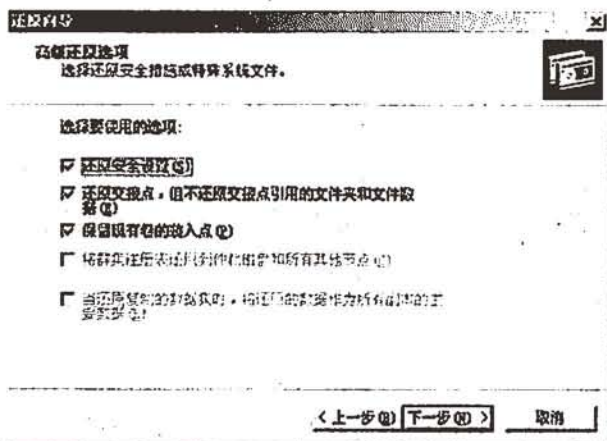


图 5.25 【高级还原选项】界面

(7) 设置好还原安全措施后，单击【下一步】按钮，打开【完成还原向导】界面，如图 5.26 所示。



图 5.26 【完成还原向导】界面

(8) 单击【完成】按钮，系统打开【还原进度】对话框并开始还原，在该对话框中显示还原的进度。还原完成后，在该对话框中将显示还原的各项状态，单击【关闭】按钮完成备份文件的还原，系统返回到【备份工具】对话框。

## 2. 文件和文件夹的简单还原

在备份和还原操作中，文件和文件夹的备份、还原使用最为普遍。下面就介绍一下简单还原文件、文件夹操作的基本功能和步骤。

### (1) 选择要还原的文件和文件夹

备份实用程序在备份时提供了文件和文件夹的树状视图，可以使用该树状视图选择要还原的文件和文件夹。这种树状视图的使用方法与 Windows 资源管理器的使用方法相同，

可以从中直接打开驱动器和文件夹,然后选择要还原的文件。

#### (2) 选择还原位置

备份实用程序允许用户选择以下 3 种目标之一作为还原的文件:

① 可以把备份的数据还原到原来的文件夹或备份时数据所在的文件夹。对还原已经受到损坏或丢失的文件和文件夹,该选项是非常有效的。

② 可以把备份的数据还原到另一个文件夹。如果选择这个选项,备份文件夹的结构和其中的文件保留在另一个文件夹中。如果用户已经知道将需要还原某些旧文件夹,但不想覆盖或改变磁盘上的当前文件或文件夹,使用此选项是非常有效的。

③ 可以把备份的文件还原到单一文件夹中。使用此选项不保留备份文件夹和文件的结构,只在单一文件夹中存放所有备份文件。如果正在查找某个文件但又不知道它的位置,这时使用该选项非常有效。

#### (3) 设置还原选项

备份实用程序在【选项】对话框中为我们提供了如何还原的选项设置,利用该对话框可以选择还原文件和文件夹的各种方法。为此必须选择以下 3 个选项之一:选择【保留现有文件】单选按钮后,可以防止硬盘上的文件被覆盖。这是还原文件最安全的一种方法。

选择【如果现有文件比备份文件旧,将其替换】单选按钮后,如果自从最后一次备份数据以来已经损坏了文件,此选项可以保证对文件所作的修改丝毫不损。

选择【替换现有文件】单选按钮后,即用备份集中的文件替换硬盘上的全部文件。如果自从最后一次备份数据以来已经对数据做过修改,该选项将删除这些修改。

#### (4) 开始还原操作

当开始还原操作时,备份实用程序将提示用户确认是否已经做好数据还原的准备,此时还有机会设置高级还原选项,包括是否想恢复安全设置、活动存储设备数据库和连接点数据等。

用户既可以使用备份实用程序以 FAT 容量备份和还原数据,也可以以 NTFS 容量备份和还原数据。然而,如果已经在 Windows Server 2003 中使用 NTFS 容量备份了数据,该备份实用程序推荐将数据还原成在 Windows Server 2003 中使用的 NTFS 容量,否则可能会丢失数据及某些文件和文件夹特性。例如,如果在 Windows Server 2003 中使用 NTFS 容量备份数据,然后将其还原成在 Windows 2000 中使用的 FAT 容量或 NTFS 容量,那么许可文件、加密文件系统(EFS)设置、磁盘配额信息、已安装的驱动器信息和远程存储器信息等都将丢失。

如果还原“系统状态”数据,并且不具体为还原的数据指定可替换的位置,那么备份实用程序将删除该“系统状态”数据。这时该“系统状态”数据当前位于计算机上,并用正在还原的“系统状态”数据替换它。同样,如果将“系统状态”数据还原到一个可替换位置,那么只有注册表文件、SYSVOL 目录文件和系统引导文件还原到该可替换位置。如果指定了一个可替换的位置,则活动文件夹目录服务数据库、验证服务数据库和 COM+类注册数据库不能还原。

为了还原域控制器上的“系统状态”数据,必须首先以目录服务还原模式启动计算机。这样才允许还原 SYSVOL 目录和活动目录。用户只能还原本地计算机上的“系统状态”数据,而不能还原远程计算机上的“系统状态”数据。管理员和备份操作者不必解密文件和

文件夹就可以还原加密的文件和文件夹。

#### 5.3.1.4 Windows Server 2003 的备份作业计划

用户可以事先为备份制订作业计划，确定了备份的日期和时间后，当系统时间到指定的时间时，可自动按事先设定的备份选项和安排进行备份。

下面是设定备份作业计划的具体操作步骤。

(1) 在【备份工具】对话框中，单击【计划作业】标签打开【计划作业】选项卡，如图 5.27 所示。

(2) 在【计划作业】选项卡中，单击【添加作业】按钮将打开如前图 5.4 所示的【备份向导】的欢迎画面，从中单击【下一步】按钮，打开如前图 5.5 所示的【要备份的内容】界面，从中选择要备份的资料类型。

(3) 单击【下一步】按钮，打开如前图 5.6 所示的【备份类型、目标和名称】界面，从中确定了备份媒体类型和文件名后，单击【下一步】按钮打开【如何备份】界面，在此对话框中可设置在备份后是否进行验证。

(4) 然后单击【下一步】按钮，打开【备份选项】界面。在该界面中可以指定是否要改写数据还是限制对数据的访问。然后单击【下一步】按钮打开【备份标签】界面，在该界面中需要指定备份的标签和正在使用的标签。然后单击【下一步】按钮，在打开的界面中可指定是现在运行备份还是以后再运行。若指定以后再运行，可选中【以后】单选按钮，此时在【作业名】文本框中输入该作业的名称。

(5) 然后单击【下一步】按钮，打开【完成备份向导】界面，从中单击【完成】按钮，系统返回图 5.27 所示的【计划作业】选项卡。至此，一个备份作业计划就设定完成了。



图 5.27 【计划作业】选项卡

#### 5.3.1.5 Windows Server 2003 的备份操作者和用户权限

为了系统的安全和操作的可靠性，必须对备份和还原操作设置必要的访问权限，这样

可以防止未经授权擅自闯入者的破坏而造成数据的损失和泄密。为此, Windows Server 2003 对系统备份和还原提供设置用户访问权限的功能。

#### 1. 普通用户

普通用户可以备份自己的文件或具有读/写权限的文件,但在要恢复时只能替换自己的文件或具有写权限的文件,对于只读权限的文件只能使用重定向恢复。

#### 2. 系统管理员组、备份操作员组和服务员操作员组的用户

系统管理员组(Administrators)、备份操作员组(Backup Operators)和服务员操作员组(Server Operators)的用户可以不受权限的限制,可以备份所有文件和系统状态,也可恢复所有文件和系统状态。

### 5.3.2 典型例题分析

例 阅读以下说明,回答问题 1~4,将解答填入对应的答案栏内。

#### 【说明】

A 公司有一台 Windows Server 2003 服务器,配有一个磁带机用于数据备份。该公司建立了完善的数据备份制度:每个工作日的深夜都要对数据进行一次备份,且每天都使用单独一盘磁带用于数据备份,磁带编号分别为 NO.1、NO.2、…、NO.5。数据备份策略如表 5.3 所示。

表 5.3 A 公司数据备份策略

项目	星期一	星期二	星期三	星期四	星期五
备份方式	正常备份	差异备份	差异备份	差异备份	差异备份
所用磁带	NO.1	NO.2	NO.3	NO.4	NO.5

【问题 1】备份的目的是什么?

【问题 2】差异备份与增量备份有什么相同点?有什么不同点?

【问题 3】如果在星期五中午出现数据丢失,要进行数据恢复,请问需要哪几盘磁带才能恢复到星期四备份时的数据?

【问题 4】某一天该服务器受到网络黑客的攻击,某个文件夹中的一些文件被篡改了(具体是哪些文件还不清楚)。当用户发现时,这个文件夹的有些文件已经被合法地修改过。这时要恢复被篡改的文件,最好使用哪种数据恢复策略?

分析:该题主要考查考生对数据备份和恢复策略的理解。

问题 1:数据备份是设计用来保护系统,防止由于硬件或媒体失效或者其他损坏事件的故障而丢失数据。如果系统中的数据丢失,则可通过备份实用程序就可以方便地从存档的拷贝中恢复数据,同时能将系统从各种故障中恢复正常运行。

问题 2:为了提高备份速度,在备份数据时只备份自从最后一次正常备份或增量备份以来创建或经过修改的文件,而不是全部文件。备份这些文件有两种方式,一种是差异备份,另一种是增量备份。但这两种方式是有区别的,若采用差异备份方式,它不对被备份的每一个文件都做标记,即不设置档案文件的位,换句话说,对已经做了差异备份的文件,



再进行差异备份或增量备份时还将被备份；若采用增量备份方式，则对每一个被备份的每一个文件都做标记，即设置档案文件的位，换句话说，对已经做了增量备份文件，再进行差异备份或增量备份时将不会被备份。

问题 3：该公司的备份策略是周一进行正常备份，周二至周五进行差异备份。这就是说周一将备份所有内容并修改备份标记；周二备份的内容是周二所创建或经过修改的文件；周三备份的内容是周二和周三所创建或经过修改的文件；周四备份的内容是周二、周三和周四所创建或经过修改的文件；周五备份的内容是周二至周五所创建或经过修改的所有文件。因此，当周五中午出现数据丢失，只需周一备份内容(存放在磁带 NO.1 中)和周二、周三和周四所创建或经过修改的文件的备份内容(存放在磁带 NO.4 中)就可以恢复到周四备份时的数据。

问题 4：数据恢复操作通常可以分为三类。第一类是全盘恢复，第二类是个别文件恢复，第三类是重定向恢复。若采用全盘恢复和个别文件恢复将会把该文件夹中所有文件被替换成备份时的内容，这会将那些被合法修改的内容覆盖。因此最好使用重定向恢复，即把该文件夹的所有内容恢复到另外一位置并且不覆盖该文件夹，然后采用比对的方法来恢复被篡改的文件。

答案：

【问题 1】在由于硬件或媒体失效或者其他损坏事件的故障而丢失数据时进行数据恢复。

【问题 2】共同点是只备份自从最后一次正常备份或增量备份以来又创建或修改过的文件；不同点是差异备份后不将文件标记为已经做过备份，而增量备份后将文件标记为已经做过备份。

【问题 3】NO.1 和 NO.4。

【问题 4】重定向恢复。

### 5.3.3 同步练习

1. 正常备份与复制备份有什么相同点？有什么不同点？
2. 某公司的数据备份策略如表 5.4 所示：

表 5.4 某公司数据备份策略

项目	星期一	星期二	星期三	星期四	星期五
备份方式	正常备份	增量备份	增量备份	增量备份	增量备份
所用磁带	NO.1	NO.2	NO.3	NO.4	NO.5

假设每天备份时间都是在深夜，且每天都使用单独一盘的磁带进行备份，磁带编号分别为 NO.1、NO.2、…、NO.5。如果在星期四中午出现数据丢失，要进行数据恢复，请问需要哪几盘磁带才能恢复到星期三备份时的数据？

3. 当一个已经做了备份的服务器硬盘坏了，在安装了新硬盘后需要重新恢复数据，最好使用哪种恢复策略？
4. 当一个已经做了备份的文件被病毒破坏了，要想恢复它最好使用哪种恢复策略？

5. 在 Windows Server 2003 中, 数据备份必须有哪些用户来完成? 自己能不能备份属于自己的文件?

6. 系统管理员能否在远程计算机备份某台 Windows Server 2003 计算机的系统状态数据?

### 5.3.4 同步练习参考答案

1. 共同点是将选定的文件都备份下来; 不同点是正常备份后将所有文件标记为已经做过备份, 而复制备份后不将文件标记为已经做过备份。

2. NO.1、NO.2、NO.3。

3. 全盘恢复。

4. 个别文件恢复。

5. 系统管理员组、备份操作员组和服务器操作员组的用户; 可以。

6. 不可以。

## 5.4 系统性能分析

### 5.4.1 考点辅导

#### 5.4.1.1 网络性能评价概述

随着计算机网络数量的增长、规模的扩大, 网络性能成为一个十分重要的问题。与度量单机性能不同的是, 它是度量一组计算机系统的性能。另一方面对于小规模的网络来说, 故障隔离比较简单, 而对于大规模的网络, 故障自动隔离和性能监控就显得十分必要, 也十分复杂。了解网络用户的需要, 设定恰当的性能指标, 以便更好地选择网络结构和组成, 方能得到满足用户需求, 性能价格比高的网络。

一般来说, 了解网络性能有如下用处:

- 选择和配置合适的网络产品;
- 设计整个网络;
- 管理网络;
- 评价网络;
- 网络故障检测和排除;
- 规划今后网络的发展。

#### 1. 网络性能度量

为了评价网络性能, 需要选择一些性能准则, 它能衡量网络性能品质, 而性能准则的选择又取决于网络用户的应用和需求。

从网络用户的观点来考虑, 网络性能的度量要反映对网上用户如何有效地服务, 如何快速地完成和网络有关的任务。不同的用户有不同的期望, 这主要取决于他们的应用和需求。

例如, 对交互式的应用, 最重要的网络性能是响应时间, 即从网络终端用户提出请求

到完成任务得到响应的整个时间；对经常需要批量传输数据的应用，最重要的网络性能是吞吐量，即在给定时间内能传输的数据总量。

从网络管理员的观点来考虑，他的职责是观察网络的运行、监控它的性能以保证网络的正常运行，配置和调整网络以维持用户要求的性能水平，以及根据用户需要和通信类型的改变重新配置网络资源。网络管理员最关心的网络性能是网络资源利用率，即整个运行期间资源忙所占的百分比。

由此可见，网络用户最关心的网络性能是获得最快的响应，网络管理员最关心的网络性能是获得最高的资源利用率，两者需要很好的平衡。这种平衡包括两个方面，一方面是性能和价格的折中，另一方面是吞吐量和响应时间的平衡。

影响网络性能最重要的可变参数是网络负载或通信的密度，当网络负载增加到一定程度，网络性能会下降，应使这种下降比较平滑地产生，防止突然影响性能。当网络负载增加到饱和点时，则形成瓶颈，大大增加延迟，导致阻塞。

度和评价响应时间时，需要考虑以下几方面：

- 设定一个有效的采样区间，以便能充分反映网络响应的性能；
- 在实际的网络负载条件下进行度量；
- 每次测量在相同条件下进行，以便能有效地比较；
- 采用一致的方法度量；
- 没有其他作业和网络作业竞争系统资源。

## 2. 响应时间

对一个网络环境下的信息查询系统进行网络延时测量可以分成以下三步：

- 测量在本地进行查询的响应时间；
- 通过网络在远地进行同样的查询，测量其响应时间；
- 上述两次测量的结果之差即为网络延迟，对于传送一个文件的响应时间可用下述公式计算：

$$R = A + (P \times S)$$

式中， $R$  为响应时间； $A$  为存取时间（例如，在源节点和目的节点之间建立网络连接所需时间）； $P$  为每个数据块进行处理、存取盘以及在链路间传送文件所需时间； $S$  为文件大小，以数据块为单位。

测量复制一个空文件所需的时间可得到  $A$  的值。此以下方法可得到  $P$  的值：

- 测量传输不同大小文件所需时间，得到响应时间和文件大小的函数关系，如图 5.28 所示。
- 在图中选择不同文件大小的两点 ( $S_1$  和  $S_2$ )，以及对应的传输时间 ( $t_1$  和  $t_2$ )；
- 按下式求得  $P$ ：

$$P = (t_1 - t_2) / (S_1 - S_2)$$

影响响应时间的因素来自三个部分：本地系统、网络和远程系统。一般来说，响应时间取决于在这三个部分处理通信数据的元件特性、源节点和目的节点的负载以及网上的通信量。

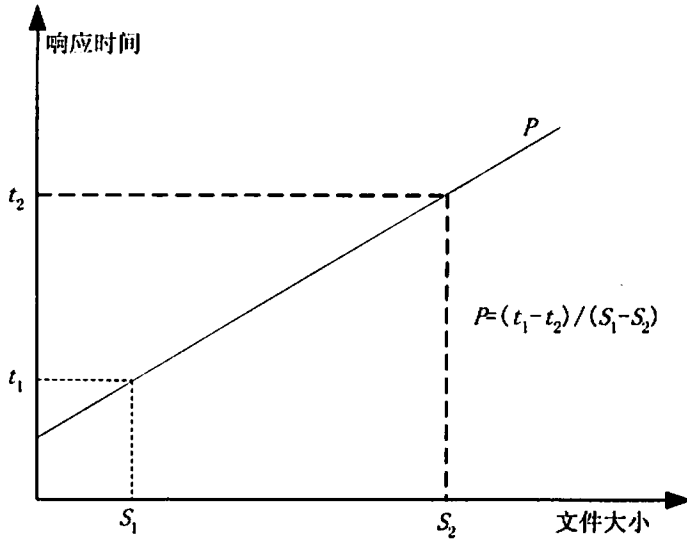


图 5.28 响应时间和文件大小的函数关系

在源节点和目的节点影响响应时间的因素有：

- CPU 的容量以及可给网络使用的时间；
- 系统的类型，如分时系统或专用系统；
- 在源节点的终端线速度；
- I/O 处理能力；
- 缓冲区的大小；
- 报文大小；
- 内存访问优先调度和存取速度。

在网络层，主要有以下三个因素：

- 协议处理的开销；
- 通信密度即网络负载；
- 传输时间。

此外，网络的规模、网络拓扑结构的复杂性、路由器的容量，传输误差和重传机制、交换系统特性等都对响应时间有影响。

为了改变网络的响应时间特性，通常采用网络硬件和网络资源升级、调整负载、调整应用以及实现分布式处理等方法。

### 3. 吞吐率

吞吐率是度量网络传输数据的能力，是单位时间内网上总的通信量。

测量和评价吞吐率的最简单的方法是用端到端的用户吞吐量除以整个传送数据的时间，并考虑传送误差的因素，通常：

$$\text{吞吐率} = M \times (1 - P) / (M / S + t)$$

式中， $M$  为报文长度，以位计； $P$  为误码率； $S$  为线速度，以每秒位计； $t$  为报文间的空闲时间，以秒计。

吞吐率的估算方法通常有以下三种。



## (1) 方法 1:

$$T = U \times (1 - E) \times S$$

式中,  $T$  为吞吐率;  $U$  为每个报文内用户数据和总数据量之比;  $E$  为报文重传的概率;  $S$  为线速度。

## (2) 方法 2:

$$R = A + (P \times B)$$

$$P = (R - A) / B$$

$$T = B / (R - A)$$

式中,  $R$  为响应时间;  $A$  为存取时间;  $P$  为数据块处理、磁盘存取及传送文件所需时间;  $B$  为文件含的数据块数。

## (3) 方法 3:

在固定速率的链路上传送一个大的文件, 测量传送时间, 估计实际的用户吞吐率。

影响吞吐率的主要因素有:

- 处理通信数据的硬件频宽或容量;
- 处理通信数据的通信软件效率;
- 在源系统和目的系统的负载;
- 网上的通信量。

## 4. 资源利用率

资源利用率用以度量资源忙的时间所占的百分比, 是评价网络性能价格比的关键数据。通常有总利用率和净利用率两类, 总利用率是用户数据处理和开销一起占总容量的百分比, 净利用率也称有效利用率, 是用户数据处理占总容量的百分比。

$$\text{有效利用率} = \text{实际吞吐率} / \text{名义吞吐率}$$

利用率、吞吐率和响应时间之间没有一个固定的关系, 需要找到一个合适的平衡关系, 通常一个大容量的网络利用率往往被网内一个小容量的组成部分所限制, 从实际经验看, 网络利用率平均为 30% 比较合适, 这样可以保证在高峰负载时仍有足够的频宽提供给用户。

资源的利用率包括 CPU 利用率、传输线路利用率、内存利用率、磁盘利用率以及网络利用率。

如果 CPU 不能提供足够的容量来处理网络任务, 则 CPU 就成了瓶颈, 通常 CPU 利用率为 30%~60%, 超过这个数时, 网络的性能会急剧下降。采用以下方法可改善 CPU 的利用率:

- 调整系统和网络;
- 调整负载;
- 重新设计某些应用;
- 控制终端 I/O 对 CPU 的并发要求以及使用好的终端 I/O 技术;
- 提高 CPU 的容量。

传输线路利用率取决于下列因素:

- 线路容量和负载;

- 通信协议和通信设备;
- 线路噪音和传输误差;
- 报文大小。

改善线路利用率的方法主要有:

- 提高 CPU 的吞吐率以改善调整线路的利用率;
- 采用效率高的通信协议以改善低速线路的利用率;
- 使用多路复用器和集中器。

网络利用率是总数据流与理论最大数据流之比,即网络成功地传递的通信总量对网络能携带的最大通信量之比。

影响网络通道利用率的两个主要因素是分配至通道的网络数据流和网络容量不一致;各个通道之间数据流和容量之比的差异很大。

改善网络利用率的措施是减少上述的不一致和差异,采用适当的流控机制。

#### 5.4.1.2 提高局域网性能的方法

当网络开始运行较慢时,提高网络运行速度可能会很困难。但可以采用几种可行的方式来提高网络性能,主要包括:减少信息流量、增加子网数目和提高网络速度 3 种方式。本节对这 3 种提高网络性能的方式进行介绍。

##### 1. 减少信息流量

当环境允许时,减少信息流量的方式是最好的。这是因为不论当前网络的结构如何,这种方式都会起作用,而且并不需要任何物理改变。减少信息流量也许意味着本地化部门子网中的服务器,或者把网络应用程序迁移到较低带宽的 Internet 客户机服务器协议。

无系统的方式减少网络信息流量必须使用工具监控网络,决定是否减轻网络上的信息流量负荷。可以查看以下几个问题区域:

(1) 产生过量信息流量的用户并查找其过量的原因,如果并没有有效的与工作相关的理由,则应该鼓励那些用户停止使用网络。

(2) 运行 Windows 的无盘工作站,这些 Windows 无盘工作站产生了网络上的巨大负荷。硬盘的价格与网络升级费用相比是很便宜的,所以考虑为那些无盘工作站计算机添加硬盘,并从本地硬盘上引导操作系统。

(3) 争取存储在真正客户机/服务器应用网络上的数据逐年地降低。例如,有时需要把一个存储在服务器上的 Access 数据库迁移到使用 Access 前端客户机应用程序与后端 SQL Server 的客户机/服务器数据库。

减轻网络负荷通常包括找出产生最大网络负荷的计算机,确定该计算机产生如此大的网络负荷的原因,如果可能的话可减轻由某一具体计算机所产生的网络负荷。重复执行以上过程,直到不可能进一步减轻网络负荷时为止,这样就把网络信息流量降至某种可行的程度。

##### 2. 增加子网数目

增加子网数目的方式是次要的方式。这种方法等价于构建更多的通路,从而可以减轻信息流量拥塞,而不是仅仅提高速度限制。除非网络远远落后于信息流量的要求,否则简

单地将该共享介质型网络拆分成多个由网桥、路由器或者执行路由服务的服务器所连接的子网,将能够从中获得诸多好处。

与高速公路网相比,拆分网络与建设更多的高速公路在道理上相同。从理论上讲,冲突域的数量加倍也就减少了每部分一半的信息流量。然而,这种方法仅仅可用于保证转换双方都处于同一子网络的情况。例如,如果拆分了网络,而网络上花费大多数时间进行通信的计算机处于不同的子网上,那么就还没有解决问题。这两台计算机的信息流量将仅仅在两个子网上进行传输。

通常情况下,把一台交换式以太网交换机(Ethernet Switch)放置于许多 Ethernet 子网段的核心,是一种能拆分网络与重连接网络,而又不会花费许多时间改变网络体系结构的易行又可以解决问题的方法。确保把子网段中的服务器用于效率最高的地方。

必须确保把花费时间互相通信的计算机单独放置于同一子网上,这也是为什么要基于一些真实个体组织拆分子网的原因。例如,按部门拆分子网通常效果很好。处于同一子网上的那些计算机用户将花费大多数时间进行子网内部的通信。

客户机/服务器局域网中绝大多数的网络信息流量的在客户机与服务器两者之间。对等型网络中能与网络上的任何其他计算机进行通信,因此网络拆分比较困难。然而,大多数客户机花费它们的大多数时间只与单个服务器进行通信,所以通常可以简单地使服务器成为每个子网的一部分。

在网络中存在多台服务器时这种方案并不容易实现,但是仍然可以识别每台客户机通常与哪台服务器进行通信,而把那台客户机放置于该服务器的子网上。然后,通过把所有服务器连接到单一高速子网,以便于通过更高速链路与其他服务器路由任何信息流量,而不是升级整个网络的链路技术。

当客户机必须访问许多不同的服务器而不指定某台服务器时,也许需要在高速主干网上实现多个服务器,使用专用的路由器连接客户子网络。这种网络结构存在需要连接到主干网络的昂贵的路由器的缺点。这也意味着每个传输到服务器的信息包都必须穿过主干网络,迫使主干网处理网络上的绝大多数信息流量。

一些环境中,客户机不仅仅要访问其部门级服务器,而且也需要访问许多其他服务器(例如,Intranet 服务器、信息传递服务器及 Internet 网关等)。虽然一种显而易见的解决方案是,把所有服务器集中于主干网络上并提供到那些服务器的路由,但是这样的配置也许效率更优,即把客户机直接连到其部门级服务器,而使用其部门级服务器提供到包含其他服务器的主干网络的路由。注意,剔除主干网的每个信息包都会使主干网运行速度更快。例如,拥有 4 台部门级服务器的网络,将能够处理其客户机请求的 25%,这些请求不需要向前转发至主干网,这样将减少主干网一半的信息流量。由于这种方法所减少的网络负荷,使当前网络在必须迁移到更高速网络技术之前多延长好几年的寿命。

路由是服务器显示的性能暗示。无论何时配置服务器执行路由功能时,都应该周期性地监控这些执行路由功能的服务器,以确保这些服务器不会导致显著的网络瓶颈。如果这些服务器真的导致了网络瓶颈,那么应该把服务器移到部门内部,而使用一台专用的桥或路由器执行路由功能。



### 3. 提高网络速度

提高速度的方式对于提高网络速度也能起到作用很好的,但是费用也很昂贵,因为这种方式需要替换网络上每种数据链路设备。用户应该视这种方式为主要的网络体系结构改变方式,在一段时间内逐渐地落实。

如果不再可能减少信息流或者有效地拆分子网,那么将不得不更新物理数据链路网络协议。通常,这种升级就是指从以太网(Ethernet)或令牌环网(Token Ring)升级到快速以太网(Fast Ethernet)或者千兆以太网。虽然这种方式比较昂贵,但用户可以不升级整个网络,也许仅仅升级主干网技术、服务器之间的链路或者某个子网至更高速网络就可以了。使用网络监视器识别网络上的大信息量的用户,并首先把那些用户迁移到更快的协议上。

## 5.4.2 典型例题分析

**例 1** 某一单位有 150 多台计算机,网络每天都会瘫痪一到三次。通常情况下,只需将一级交换机的网线全部拔出后再连上,即可恢复正常,而有时则不得不重新启动一下交换机。把原来的 10Mb/s 的网卡更换为 10/100Mb/s 网卡后,有近一个星期的时间网络没有瘫痪。然而,这几天网络又开始不正常了(已排除病毒的原因)。集线设备采用 16 口和 24 口的 10/100Mb/s 交换机,代理服务器采用 WinGate。请问这一现象的原因是什么?如何解决?

**分析:**在排除了病毒向网络疯狂发送数据包的可能后,可以认为这是典型的由广播风暴导致的网络瘫痪。广播风暴爆发后,网络中传输的全部是广播包,计算机处理的也都是广播包,正常的数据包无法得到转发和处理。拔掉网线或关掉交换机后,广播风暴得到扼制,从而恢复正常通信。

广播可以理解为一个对在场的所有人说话。这样做的好处是通话效率高,信息一下子就可以传递到网络中的所有计算机。即使没有用户人为地发送广播帧,网络上也会出现一定数量的广播帧。需要注意的是,广播不仅会占用大量的网络带宽,而且还将占用计算机大量的 CPU 处理时间。广播风暴就是网络长时间被大量的广播数据包所占用,使正常的点对点通信无法正常进行,其外在表现为网络速度非常慢,甚至导致网络瘫痪。

导致广播风暴的原因有很多,一块故障网卡或者一个故障端口都有可能引发广播风暴。

需要注意的是,交换机只能隔离碰撞域,而不能隔离广播域。事实上,当广播包的数量占到通信总量的 30% 时,网络的传输效率就会明显下降。

通常情况下,在采用多种通信协议的网络中,计算机不应多于 100 台,在采用一种通信协议的网络中,计算机不应多于 150 台。如果计算机的数量较多,应采用划分 VLAN 的方式将网络分隔开来,将大的广播域划分为若干个小的广播域,以降低广播风暴可能造成的危害。

**答案:**广播风暴;划分 VLAN(虚拟局域网)

**例 2** 某公司有一个局域网,通过交换机和 Hub 相连,近期发现网络速度变慢,但网络是连通的,请分析主要原因。

**分析:**这道是一道综合性题目,主要考查考生对网络故障的排除及网络性能分析的掌



握程度。一般说来,导致网络速度变慢原因有很多,既可能是硬件原因,也可能是软件原因。但最主要有以下几个原因:

一是网线问题导致网络速度变慢。我们知道,双绞线是由四对线按严格的规定紧密地绞和在一起的,用来减少串扰和背景噪音的影响。同时,在 T568A 标准和 T568B 标准中仅使用了双绞线的 1、2 和 3、6 四条线,其中,1、2 用于发送,3、6 用于接收,而且 1、2 必须来自一个绕对,3、6 必须来自一个绕对。只有这样,才能最大限度地避免串扰,保证数据传输。不按正确标准(T568A、T568B)制作的网线,存在很大的隐患。表现为:一种情况是刚开始使用时,网络速度就很慢;另一种情况则是开始网络速度正常,但过了一段时间后,网络速度变慢。

二是网络中存在回路导致网络速度变慢。一般当网络较小,涉及的节点数不是很多,结构不是很复杂时,这种现象很少发生。但在一些比较复杂的网络中,由于一些原因经常有多余的备用线路,则会构成回路。构成回路时,数据包会不断发送和校验数据,从而影响整体网络速度,并且查找起来比较困难。当怀疑有此类故障发生时,一般采用分区分段逐步排除的方法。为避免这种情况发生,要求我们在铺设网线时一定要养成良好的习惯,网线打上明显的标签,有备用线路的地方要做好记载。

三是网络设备硬件故障引起的广播风暴而导致网络速度变慢。作为发现未知设备的主要手段,广播在网络中起着非常重要的作用。然而,随着网络中计算机数量的增多,广播包的数量会急剧增加。当广播包的数量达到 30%时,网络的传输效率将会明显下降。当网卡或网络设备损坏后,会不停地发送广播包,从而导致广播风暴,使网络通信陷入瘫痪状态。因此,当网络设备硬件有故障时也会引起网络速度变慢。当怀疑有此类故障时,首先可采用置换法替换集线器或交换机来排除集线设备的故障。如果这些设备没有故障,关掉集线器或交换机的电源后,DOS 下用“ping”命令对所涉及计算机逐一测试,找到有故障网卡的计算机,更换新的网卡即可恢复网络速度正常。网卡、集线器以及交换机是最容易出现故障引起网络速度变慢的设备。

四是网络中某个端口形成了瓶颈导致网络速度变慢。实际上,路由器广域网端口和局域网端口、交换机端口、集线器端口和服务器网卡等都可能成为网络瓶颈。当网络速度变慢时,我们可在网络使用高峰时段,利用网管软件查看路由器、交换机、服务器端口的数据流量;也可用 netstat 命令统计各个端口的数据流量。据此确认网络数据流通瓶颈的位置,设法增加其带宽。具体方法很多,如更换服务器网卡为 100M 或 1000M、安装多个网卡、划分多个 VLAN、改变路由器配置来增加带宽等,都可以有效地缓解网络瓶颈,可以最大限度地提高数据传输速度。

五是蠕虫病毒的影响导致网络速度变慢。能过 E-mail 传播的蠕虫病毒对网络速度的影响越来越严重,危害性极大。这种病毒导致被感染的用户只要一上网就不停地往外发邮件,病毒选择用户个人电脑中的随机文档附加在用户主机的通讯簿的随机地址上进行邮件发送。成百上千的这种垃圾邮件有的排着队往外发送,有的又成批成批地被退回来堆在服务器上。造成个别骨干互联网出现明显拥塞,网络速度明显变慢,使局域网近于瘫痪。因此,我们必须及时升级所用杀毒软件;计算机也要及时升级、安装系统补丁程序,同时卸载不必要的服务、关闭不必要的端口,以提高系统的安全性和可靠性。

答案：略

### 5.4.3 同步练习

1. 某公司将现有网络进行升级改造, 原有设备如图 5.29 所示, 随着公司联网设备的增多, 整个网络性能下降得越来越快。在尽量节省资金的前提下, 同时保证原有设备的充分利用, 应如何改善网络性能? 增加什么设备? 并说出理由。

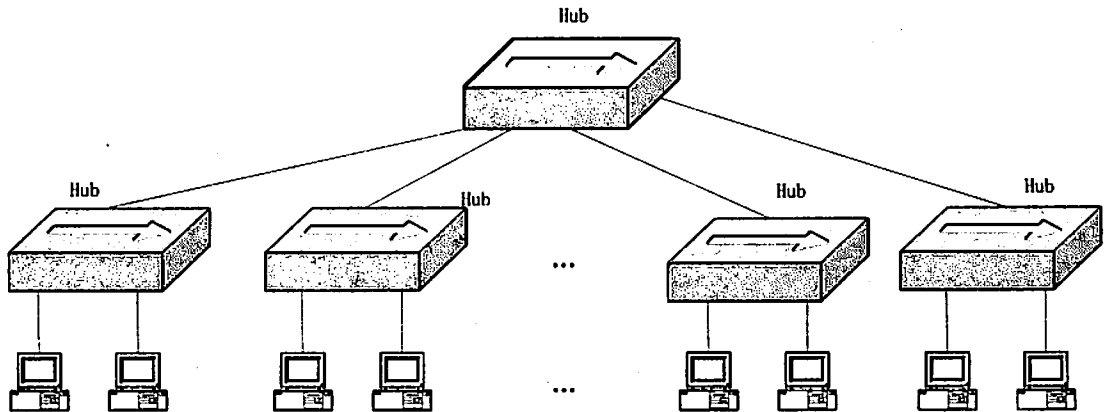


图 5.29 同步练习题 1 示意图

2. 某公司有一小型局域网, 包括一台 Windows Server 2003 服务器和 20 台客户机, 原先使用一个 10M 的 Hub 相连。随着业务增加, 该公司新购买一台 10M/100M 自适应的交换机替换下原来的 Hub, 但发现访问服务器速度并没有明显改变。请列举可能的原因, 并说明理由和解决办法。

### 5.4.4 同步练习参考答案

1. 将 Hub 换成交换机, Hub 连到交换机的一个端口上, 下连多个计算机。Hub 是共享设备, 交换机将网络分成多个网段, 多个网段间可以同时进行信息交换。

2. 可能原因有两个: 一是服务器的网卡, 网卡可能是 10M 网卡, 虽然换了 10M/100M 自适应交换机, 但服务器的接入速度仍然是 10M, 解决办法是更换 100M 网卡; 二是服务器性能, 可能是服务器的处理速度太低、内存太少或硬盘存取速度较慢, 解决办法是升级服务器或增加服务器来分担任务。

## 5.5 本章小结

这部分主要介绍了常用的网络工具的使用; 简单网络故障的分析、定位、诊断和排除; 数据备份和数据恢复; 系统性能分析原理及常用的解决办法。

大纲中对网络系统的运行、维护和管理的要求比较笼统, 主要目的是考查考生实际的网络管理和维护能力, 而这些能力只能通过实践才能获得, 很难从教科书中得到答案。正



因如此,笔者只能紧扣大纲,结合本人实际工作经验,对网络上的一些资料进行了搜集整理,以便考生复习迎考。本章的每小节中都组织了一些的针对水平考试的典型例题分析和同步训练,这些题目基本上涵盖了大纲规定的知识要点。

从2004年下半年网络管理员考试来看,本章考试份量较重,有5分(试题二的问题3)。笔者认为,考生应把复习重点放在网络故障的分析、定位、诊断和排除,但也不放松对常用的网络工具的使用、数据备份和数据恢复、系统性能分析原理及常用的解决办法的学习。

## 5.6 达标训练题及参考答案

### 5.6.1 达标训练题

1. ping 命令的“-n count”参数的含义是什么?

2. 命令“netstat -s -p TCP 60”的含义是什么?

3. 有一小型局域网,一台服务器用作 DHCP 服务器,为各客户机分配 IP 地址,有 20 台客户机,它们通过一台 24 口 Hub 相连。有一台 Windows 2000 客户机启动时无法访问 Internet,运行 ipconfig/all 命令后显示 MAC 地址为 00-00-E8-6E-24-2F,IP 地址为 0.0.0.0,子网掩码为 0.0.0.0, DHCP 服务器地址是 255.255.255.255。请列出可能出现的硬件和软件故障。

4. 某一公司的域名为 abc.com.cn,内部有一个名字为 www.abc.com.cn 的 Web 服务器所有客户机在浏览地址栏中输入 www.abc.com.cn 都无法访问内部的 Web 服务器。请问最有可能的问题是什么?

5. 某公司的数据备份策略如表 5.5 所示。

表 5.5 某公司数据备份策略

项目	星期一	星期二	星期三	星期四	星期五
备份方式	正常备份	增量备份	增量备份 复制备份	增量备份	增量备份
所用磁带	NO.1	NO.2	NO.3/NO.6	NO.4	NO.5

假设每天备份时间都是在深夜,且每天都使用单独一盘的磁带进行备份,磁带编号分别为 NO.1、NO.2、…、NO.5。为了提高备份可靠性,该公司决定在星期三在进行增量备份后增加一次复制备份,所使用的磁带编号为 NO.6。如果在星期五中午出现数据丢失,要进行数据恢复,请问需要哪几盘磁带才能恢复到星期四备份时的数据?(列举出两种方法)

6. 为了演练在灾难发生时能迅速恢复数据,需要将备份的内容恢复到计算机中,应当使用怎样的恢复策略?

7. 某公司有一个局域网,采用 100M 全交换结构,拓扑如图 5.30 所示。但随着用户数的增加,整个网络性能下降得越来越快。在尽量节省资金的前提下,同时要保证原有设备的充分利用,应如何改善网络性能?需要增加什么设备?并说明理由。

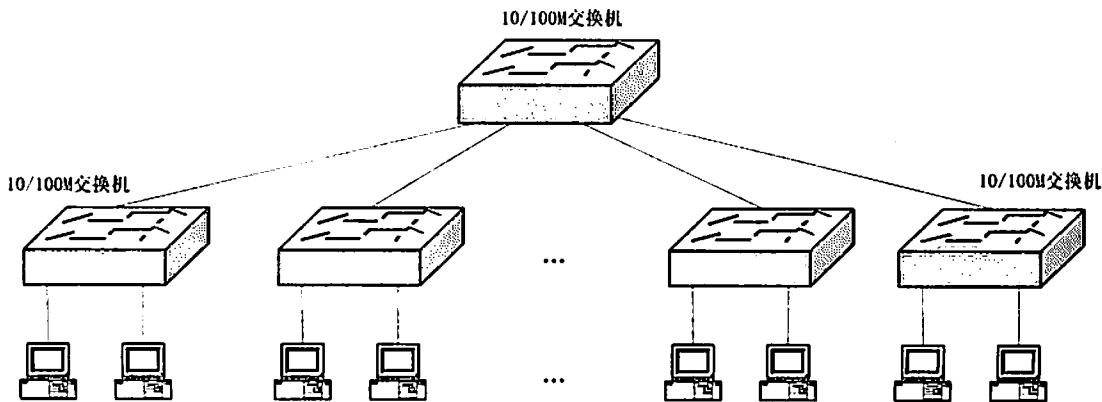


图 5.30 达标训练题 7 示意图

8. 有一台 Windows Server 2003 现在正作为文件服务器，而且用户开始抱怨访问服务器的文件越来越慢。在服务器上的用户数目没有增加，并且没有任何附加应用程序在服务器上运行，应该怎么样做来帮助提高访问文件的性能？

### 5.6.2 参考答案

1. 指定要 ping 多少次，具体次数由 count 来指定。
2. 每分钟统计一下本机的 TCP 连接情况。
3. 硬件故障主要有：网线、跳线或信息插座故障、Hub 电源未打开、Hub 硬件故障或 Hub 端口硬件故障；软件故障主要是 DHCP 服务器设置错误或 IP 地址资源不足，客户机无法租约到 IP 地址。
4. 域名服务器工作不正常或配置错误。
5. 方法一：NO.6 和 NO.4；方法二：NO.1、NO.2、NO.3 和 NO.4。
6. 重定向恢复。
7. 划分 VLAN(虚拟局域网)；购买路由器；交换环境只能减少冲突域的大小，而没有减少广播域的大小，在网络中计算机数量的增多，广播包的数量会急剧增加，网络的传输效率将会明显下降。通过划分 VLAN(虚拟局域网)减少广播域的大小，但 VLAN 之间数据交换需要路由器。
8. 整理卷碎片。



## 第6章 网络安全技术

大纲要求:

- 网络病毒防护策略
- 防火墙的配置策略
- 入侵处理策略
- 漏洞处理策略

### 6.1 网络病毒防护策略

#### 6.1.1 考点辅导

##### 6.1.1.1 网络病毒简介

###### 1. 什么是网络病毒

网络病毒是在网络上传播的计算机病毒,可能会为网络带来灾难性的后果,被称之为“二代病毒”。

###### 网络病毒的特点

网络病毒的特点及危害性主要表现在:破坏性强、传播性强、具有潜伏性和可激发性、针对性强、扩散面广、传播速度快、难以彻底清除等。

##### 6.1.1.2 基于网络的防病毒系统

###### 1. 网络防病毒需求

目前,Internet 已经成为病毒传播的最大途径,电子邮件和网络信息的传递为病毒传播打开了高速的通道。各行各业网络化的发展也使病毒的传播速度大大提高,感染的范围也越来越广。可以说,网络化带来了病毒的高效率,而病毒的高效率也对防病毒产品提出新的要求。

###### 2. 网络病毒其传播方式

一般来说,计算机网络的基本构成为网络服务器和网络节点站(包括有盘工作站、无盘工作站和远程工作站)。计算机病毒一般首先通过有盘工作站传播到软盘和硬盘,然后通过网络,进一步在网上传播。具体来说,其传播方式有如下几种:

- (1) 病毒直接从有盘工作站复制到服务器中。
- (2) 病毒先传染工作站,在工作站内存驻留,等运行网络盘内程序时再传染。
- (3) 病毒先传染工作站,在工作站内存驻留,在运行时直接通过映像路径传染。
- (4) 如果远程工作站被病毒侵入,病毒也可以通过通信过程中的数据交换传播。

服务器中。

### 3. 网络病毒防护策略

基于网络系统的病毒防护体系主要包括以下几个方面的策略:

#### (1) 防毒一定要实现全方位、多层次防毒

一定要部署多层次病毒防线,如网关防毒,群件服务器、应用服务器防毒和客户端防毒,保证斩断病毒可以传播、寄生的每一个节点,实现病毒的全面防范。

#### (2) 网关防毒是整体防毒的首要防线

将网关防毒作为最重要的一道防线来部署,全面消除外来病毒的威胁,使得病毒不再从网络传播进来,对内部网资源和系统资源造成消耗。同时,网关防毒这道防线还必须具备内容过滤功能,全面防范垃圾邮件的侵扰以及内部机密数据的外泄。

#### (3) 缺乏管理的防毒系统是无效的防毒系统

为保证防毒系统有效、及时地拦截病毒,必须确保整个防毒产品可以从管理系统中及时得到更新,整个系统中任何一个节点都可以被管理人员随时管理。

#### (4) 技术支持服务是整体防毒系统中极为重要的一环

病毒破坏系统的方法多种多样、病毒传播和感染的多种手段、新的病毒对防病毒软件自身破坏情况的增多,这些都造成防病毒软件在具体实施和应用中会遇到各种各样的问题。因此,防病毒厂商能否及时、全面地提供解决方案及技术支持服务是能不能对网络病毒进行有效防范极为重要的一环,另一方面要求厂商能有足够的本地化技术人员作为依托。

### 4. 网络防毒系统组织形式

#### (1) 系统中心统一管理

为了提高杀毒的效率和稳定性,可采用多级管理体系,由系统中心统一管理。以控制网络内的所有的机器统一杀毒,在同一时间查杀所有病毒,从而解决网络中服务器的重复感染问题。

#### (2) 远程安装升级

网络病毒防护系统提供远程安装和用户通过 Web 页面下载客户端自行安装,客户端能自动从系统中心升级。

#### (3) 一般客户端的防毒

系统中心可以控制客户端的杀毒软件,由系统中心统一组织杀毒,客户端也可自行查杀,并将结果报送系统中心。服务器端的查杀操作应与客户端一致,区别在于软件为服务器专门设计的杀毒软件。

#### (4) 防病毒过滤网关

防病毒过滤网关实际上就是企业级病毒防火墙,通常防病毒过滤网关通过部署在用户内部网与外部网的接入点,实现邮件病毒过滤及 Internet 病毒过滤,可以简单、高效地对用户网络可能遇到的来自 Internet 的病毒威胁提供强有力的深层病毒防护。

#### (5) 硬件防病毒网关

与客户端、服务器软件类防毒产品相比硬件防毒网关类产品具有以下特色:

- 高效稳定。由于采用独立的硬件平台,大大提高了系统的稳定性和查杀病毒的效率。
- 操作简单、管理方便。硬件防毒网关类产品一般采用 B/S 管理构架,友好的图形

因如此,笔者只能紧扣大纲,结合本人实际工作经验,对网络上的一些资料进行了搜集整理,以便考生复习迎考。本章的每小节中都组织了一些的针对水平考试的典型例题分析和同步训练,这些题目基本上涵盖了大纲规定的知识要点。

从2004年下半年网络管理员考试来看,本章考试份量较重,有5分(试题二的问题3)。笔者认为,考生应把复习重点放在网络故障的分析、定位、诊断和排除,但也不放松对常用的网络工具的使用、数据备份和数据恢复、系统性能分析原理及常用的解决办法的学习。

## 5.6 达标训练题及参考答案

### 5.6.1 达标训练题

1. ping 命令的“-n count”参数的含义是什么?

2. 命令“netstat -s -p TCP 60”的含义是什么?

3. 有一小型局域网,一台服务器用作 DHCP 服务器,为各客户机分配 IP 地址,有 20 台客户机,它们通过一台 24 口 Hub 相连。有一台 Windows 2000 客户机启动时无法访问 Internet,运行 ipconfig/all 命令后显示 MAC 地址为 00-00-E8-6E-24-2F,IP 地址为 0.0.0.0,子网掩码为 0.0.0.0, DHCP 服务器地址是 255.255.255.255。请列出可能出现的硬件和软件故障。

4. 某一公司的域名为 abc.com.cn,内部有一个名字为 www.abc.com.cn 的 Web 服务器所有客户机在浏览地址栏中输入 www.abc.com.cn 都无法访问内部的 Web 服务器。请问最有可能的问题是什么?

5. 某公司的数据备份策略如表 5.5 所示。

表 5.5 某公司数据备份策略

项目	星期一	星期二	星期三	星期四	星期五
备份方式	正常备份	增量备份	增量备份 复制备份	增量备份	增量备份
所用磁带	NO.1	NO.2	NO.3/NO.6	NO.4	NO.5

假设每天备份时间都是在深夜,且每天都使用单独一盘的磁带进行备份,磁带编号分别为 NO.1、NO.2、…、NO.5。为了提高备份可靠性,该公司决定在星期三在进行增量备份后增加一次复制备份,所使用的磁带编号为 NO.6。如果在星期五中午出现数据丢失,要进行数据恢复,请问需要哪几盘磁带才能恢复到星期四备份时的数据?(列举出两种方法)

6. 为了演练在灾难发生时能迅速恢复数据,需要将备份的内容恢复到计算机中,应当使用怎样的恢复策略?

7. 某公司有一个局域网,采用 100M 全交换结构,拓扑如图 5.30 所示。但随着用户数的增加,整个网络性能下降得越来越快。在尽量节省资金的前提下,同时要保证原有设备的充分利用,应如何改善网络性能?需要增加什么设备?并说明理由。

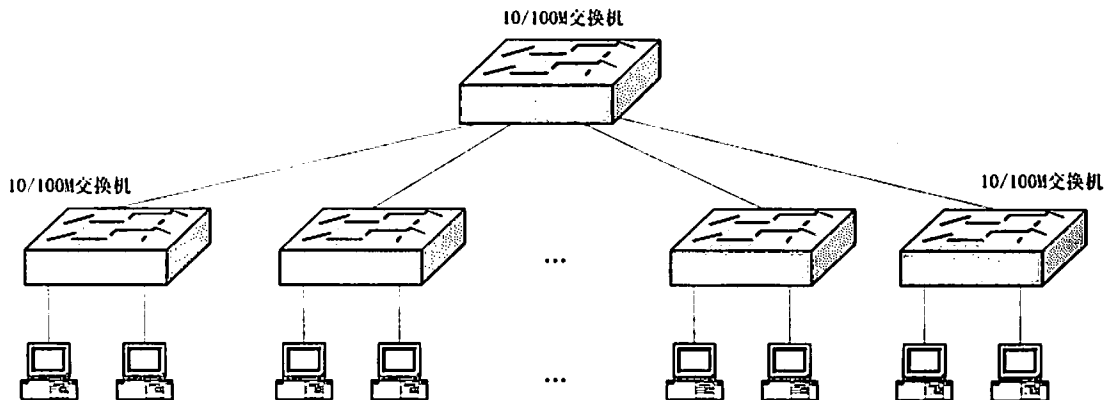


图 5.30 达标训练题 7 示意图

8. 有一台 Windows Server 2003 现在正作为文件服务器, 而且用户开始抱怨访问服务器的文件越来越慢。在服务器上的用户数目没有增加, 并且没有任何附加应用程序在服务器上运行, 应该怎么样做来帮助提高访问文件的性能?

## 5.6.2 参考答案

1. 指定要 ping 多少次, 具体次数由 count 来指定。
2. 每分钟统计一下本机的 TCP 连接情况。
3. 硬件故障主要有: 网线、跳线或信息插座故障、Hub 电源未打开、Hub 硬件故障或 Hub 端口硬件故障; 软件故障主要是 DHCP 服务器设置错误或 IP 地址资源不足, 客户机无法租约到 IP 地址。
4. 域名服务器工作不正常或配置错误。
5. 方法一: NO.6 和 NO.4; 方法二: NO.1、NO.2、NO.3 和 NO.4。
6. 重定向恢复。
7. 划分 VLAN(虚拟局域网); 购买路由器; 交换环境只能减少冲突域的大小, 而没有减少广播域的大小, 在网络中计算机数量的增多, 广播包的数量会急剧增加, 网络的传输效率将会明显下降。通过划分 VLAN(虚拟局域网)减少广播域的大小, 但 VLAN 之间数据交换需要路由器。
8. 整理卷碎片。



## 第6章 网络安全技术

大纲要求:

- 网络病毒防护策略
- 防火墙的配置策略
- 入侵处理策略
- 漏洞处理策略

### 6.1 网络病毒防护策略

#### 6.1.1 考点辅导

##### 6.1.1.1 网络病毒简介

###### 1. 什么是网络病毒

网络病毒是在网络上传播的计算机病毒,可能会为网络带来灾难性的后果,被称之为“第二代病毒”。

###### 2. 网络病毒的特点

网络病毒的特点及危害性主要表现在:破坏性强、传播性强、具有潜伏性和可激发性、针对性强、扩散面广、传播速度快、难以彻底清除等。

##### 6.1.1.2 基于网络的防病毒系统

###### 1. 网络防病毒需求

目前,Internet 已经成为病毒传播的最大途径,电子邮件和网络信息的传递为病毒传播打开了高速的通道。各行各业网络化的发展也使病毒的传播速度大大提高,感染的范围也越来越广。可以说,网络化带来了病毒的高效率,而病毒的高效率也对防病毒产品提出了新的要求。

###### 2. 网络病毒其传播方式

一般来说,计算机网络的基本构成为网络服务器和网络节点站(包括有盘工作站,无盘工作站和远程工作站)。计算机病毒一般首先通过有盘工作站传播到软盘和硬盘,然后进入网络,进一步在网上传播。具体来说,其传播方式有如下几种:

- (1) 病毒直接从有盘工作站复制到服务器中。
- (2) 病毒先传染工作站,在工作站内存驻留,等运行网络盘内程序时再传染给服务器。
- (3) 病毒先传染工作站,在工作站内存驻留,在运行时直接通过映像路径传染到服务器。
- (4) 如果远程工作站被病毒侵入,病毒也可以通过通信过程中的数据交换进入网络服

服务器中。

### 3. 网络病毒防护策略

基于网络系统的病毒防护体系主要包括以下几个方面的策略:

#### (1) 防毒一定要实现全方位、多层次防毒

一定要部署多层次病毒防线,如网关防毒,群件服务器、应用服务器防毒和客户端防毒,保证斩断病毒可以传播、寄生的每一个节点,实现病毒的全面防范。

#### (2) 网关防毒是整体防毒的首要防线

将网关防毒作为最重要的一道防线来部署,全面消除外来病毒的威胁,使得病毒不再从网络传播进来,对内部网资源和系统资源造成消耗。同时,网关防毒这道防线还必须具备内容过滤功能,全面防范垃圾邮件的侵扰以及内部机密数据的外泄。

#### (3) 缺乏管理的防毒系统是无效的防毒系统

为保证防毒系统有效、及时地拦截病毒,必须确保整个防毒产品可以从管理系统中及时得到更新,整个系统中任何一个节点都可以被管理人员随时管理。

#### (4) 技术支持服务是整体防毒系统中极为重要的一环

病毒破坏系统的方法多种多样、病毒传播和感染的多种手段、新的病毒对防病毒软件自身破坏情况的增多,这些都造成防病毒软件在具体实施和应用中会遇到各种各样的问题。因此,防病毒厂商能否及时、全面地提供解决方案及技术支持服务是能不能对网络病毒进行有效防范极为重要的一环,另一方面要求厂商能有足够的本地化技术人员作为依托。

### 4. 网络防毒系统组织形式

#### (1) 系统中心统一管理

为了提高杀毒的效率和稳定性,可采用多级管理体系,由系统中心统一管理。中心可以控制网络内的所有的机器统一杀毒,在同一时间查杀所有病毒,从而解决网络环境下机器的重复感染问题。

#### (2) 远程安装升级

网络病毒防护系统提供远程安装和用户通过 Web 页面下载客户端自行安装两种方式,客户端能自动从系统中心升级。

#### (3) 一般客户端的防毒

系统中心可以控制客户端的杀毒软件,由系统中心统一组织杀毒,客户端也可自行查杀,并将结果报送系统中心。服务器端的查杀操作应与客户端一致,区别在于软件为服务器专门设计的杀毒软件。

#### (4) 防病毒过滤网关

防病毒过滤网关实际上就是企业级病毒防火墙,通常防病毒过滤网关通过部署在用户内部网与外部网的接入点,实现邮件病毒过滤及 Internet 病毒过滤,可以简单、高效地对用户网络可能遇到的来自 Internet 的病毒威胁提供强有力的深层病毒防护。

#### (5) 硬件防病毒网关

与客户端、服务器软件类防毒产品相比硬件防毒网关类产品具有以下特色:

- 高效稳定。由于采用独立的硬件平台,大大提高了系统的稳定性和查杀病毒的效率。
- 操作简单、管理方便。硬件防毒网关类产品一般采用 B/S 管理构架,友好的图形

管理界面可供用户方便地对设备进行简便易行的配置。

- 接入方式简单易行。
- 免维护，远程自动更新代码和系统升级，无须管理员日常维护。
- 容错与集群，系统通过集群模块，在容错的同时，线性地增加处理能力，满足高带宽的网关杀毒需要。

### 6.1.2 典型例题分析

**例** 防病毒过滤网关产品由多个防毒功能模块构成，其中最重要的是什么功能？

**分析：**防病毒过滤网关实际上就是企业级病毒防火墙，可谓“一夫当关、万夫莫开”。通常防病毒过滤网关通过部署在用户内部网与外部网的接入点，实现邮件病毒过滤及 Internet 病毒过滤，可以简单、高效地对用户网络来自 Internet 的病毒威胁实现强有力的深层病毒防护。该类产品由邮件病毒过滤、网页病毒过滤和 FTP 下载过滤等几大防毒功能模块构成，其中最重要的是邮件病毒过滤功能。

**答案：**邮件病毒过滤功能。

### 6.1.3 同步练习

1. 简述网络病毒防护策略。
2. 简述网络防病毒的组织形式。
3. 简述硬件防病毒网关的特色(与客户端、服务器软件类防毒产品相比)。
4. 简述网络病毒的特点？
5. 为了防范 Internet 的病毒对企业内部网的威胁，企业内部可购置什么防护系统？此系统部署在什么地方？

### 6.1.4 同步练习参考答案

1、2、3、4 题答案见本节考点辅导。

5. 为了防范因特网的病毒对企业内部网的威胁，企业内部可购置防病毒过滤网关防护系统。此系统部署在用户内部网与外部网的接入点处。

## 6.2 防火墙的配置策略

### 6.2.1 考点辅导

#### 6.2.1.1 防火墙概述

##### 1. 什么是防火墙

防火墙是位于两个信任程度不同的网络之间的软件或硬件设备的组合，它对两个或多

个网络之间的通信进行控制,通过强制实施统一的安全策略,防止对重要信息资源的非法存取和访问,以达到保护系统安全的目的。

## 2. 防火墙的相关概念

防火墙的相关概念有:非信任网络(公共网络)、信任网络(内部网络)、DMZ(非军事化区)、可信主机、非可信主机、公网 IP 地址、保留 IP 地址、包过滤、地址转换。

- 非信任网络(公共网络):处于防火墙之外的公共开放网络,一般指 Internet。
- 信任网络(内部网络):位于防火墙之内的可信网络,是防火墙要保护的目标。
- DMZ(非军事化区):也称周边网络,可以位于防火墙之外也可以位于防火墙之内。安全敏感度和保护强度较低。非军事化区一般用来放置提供公共网络服务的设备。这些设备由于必须被公共网络访问,所以无法提供与内部网主机相等的安全性。
- 可信主机:位于内部网的主机,且具有可信任的安全特性。
- 非可信主机:不具有可信特性的主机。
- 公网 IP 地址:有 Internet 信息中心统一管理分配的 IP 地址。可在 Internet 上使用。
- 保留 IP 地址:专门保留用于内部网的 IP 地址。可以由网络管理员任意指派,在 Internet 上不可识别和不可路由,如 192.168.0.0 和 10.0.0.0 等地址网段。
- 包过滤:防火墙对每个数据包进行允许或拒绝的决定,具体地说,就是根据数据包的头部按照规则进行判断,决定继续转发还是丢弃。
- 地址转换:防火墙将内部网主机不可路由的保留地址转换成公共网络可识别的公共地址,可以达到节省 IP 和隐藏内部网络拓扑结构信息等目的。

## 3. 防火墙的特性

防火墙的功能及优点如下:

- 对进出的数据包进行过滤,过滤掉不安全的服务和非法用户。
- 监视 Internet 安全,对网络攻击行为进行检测和报警。
- 记录通过防火墙的信息内容和活动。
- 控制对特殊站点的访问,封堵某些禁止的访问行为。
- 防火墙能强化安全策略,执行系统规定的规则,仅允许符合规则的信息通过。
- 防火墙能有效的记录 Internet 上的活动。因为所有进出的信息都需要经过防火墙,所以防火墙可以记录信任网络和非信任网络之间发生的各种事件。
- 防火墙是一个安全策略的边防站,所有进出内部网的信息都必须通过防火墙,防火墙便成为一个安全检查站,能够把可疑的连接或者访问拒之门外。

防火墙具有以下缺点:

- 防火墙不能防范不经过防火墙的攻击。未经过防火墙的数据,防火墙无法检查,比如拨号上网。
- 防火墙不能解决来自内部网络的攻击和安全问题。对于防火墙内部各主机间的攻击行为,防火墙就爱莫能助。
- 防火墙不能防止最新的未设置策略或错误配置引起的安全威胁。因为防火墙的各种策略是在某攻击方式经过专家分析后给出其特征进而设置的。
- 防火墙不能防止人为或自然的破坏。防火墙是一个安全设备,但防火墙本身必须



存在于一个安全的地方。

- 防火墙无法解决 TCP/IP 等协议的漏洞。防火墙本身就是基于 TCP/IP 等协议而实现的, 因此就无法解决 TCP/IP 操作的漏洞。比如利用 DOS 或 DDOS 攻击。
- 防火墙对服务器合法开放的端口的攻击大多无法阻止。
- 防火墙不能防止受病毒感染的文件的传输。防火墙本身并不具备查杀病毒的功能, 即使集成了第三方的防病毒软件, 也没有一种软件可以查杀所有的病毒。
- 防火墙不能防止数据驱动式的攻击。当有些表面看来无害的数据邮寄或复制到内部网的主机上并被执行时, 可能会发生数据驱动式的攻击。
- 防火墙不能防止内部的泄密行为。防火墙内部的一个合法用户主动泄密, 防火墙对此是无能为力的。
- 防火墙不能防止对本身安全漏洞的威胁。防火墙保护别人有时却无法保护自己, 因为目前还没有厂商绝对保证防火墙不会存在安全漏洞。防火墙也有一个操作系统, 也有着其硬件系统和软件, 因此依然有着漏洞和 Bug。所以其本身也可能受到攻击和出现软件和硬件方面的故障。

#### 4. 防火墙的基本分类

根据防火墙实现原理的不同, 通常将防火墙分为包过滤防火墙、应用层网关防火墙和状态检测防火墙 3 类。

##### 6.2.1.2 防火墙系统安装与配置

下面主要以方正方御防火墙为例对防火墙的安装和配置进行说明。

##### 1. 软硬件安装

方御防火墙的软件部分主要由管理监控程序(FireControl)、串口配置程序(FCInit)和日志报警程序(LogService)组成。FireControl 是方御防火墙的管理程序, 其作用是管理、监控、配置方御防火墙和设置入侵攻击报警策略, 进行设备管理和日常监控; FCInit 的主要功能是初始化 FG 防火墙, 通过配置串口来完成初始化的工作; LogService 的功能是获取日志、提供日志报警信息, 在程序的安装过程中, 能够自动装载数据和文件, 并在系统程序组中, 生成方御防火墙的程序组。

方御防火墙的硬件名称为 FireGate, 简称 FG。

- 用网线将外部网接口连接 FG 的外部接口。
- 用网线将内部网接口连接 FG 的内部接口。
- 用网线将控制主机连接 FG 的控制接口。
- 用网线将开放区服务器接 DMZ 区接口。
- 用电源线将 FG 接上电源, 硬件安装完成。

其硬件安装结构如图 6.1 所示。

##### 2. 基本配置

FireControl 安装在控制机上, 控制机可以是与 FireControl 网口相连的任意台机器; 在 FireControl 安装程序完毕后, 即可在桌面上找到它的快捷方式。

管理员第一次启动 FireControl 管理程序时, 应使用在 FCInit 中新建实施域时创建的默

认账号 admin 进行登录。登录成功后,为安全起见,建议即刻修改 admin 账号的密码,以策略管理员身份登录 FireControl。策略管理员可自定义防火墙的各种参数,配置个性化的防火墙。防火墙的基本配置包括以下几个方面:

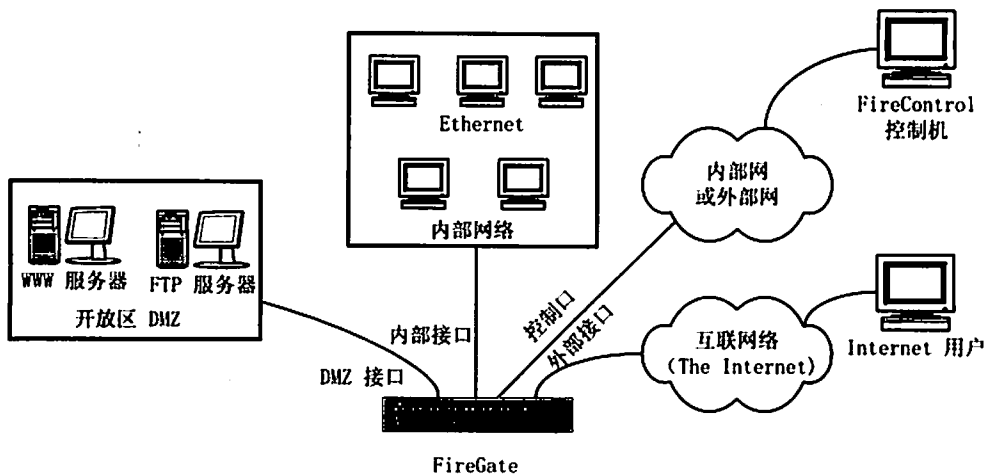


图 6.1 硬件安装结构

### (1) 别名

别名配置是为相关网络地址和端口设置别名。别名的设计是为了方便策略管理员的使用,策略管理员可以使用为记的别名代替多个功能端口以及子网,使配置不再繁琐。例如使用别名 www 代替端口 80 或 8080,别名 office 代替 IP 地址为 105.118.0.0,子网掩码为 255.255.255.0 的网段地址,或者把几个离散的端口值和网段地址统一用一个别名进行管理。

别名是 FG 防火墙中重要的特性,大部分防火墙规则的配置都是通过别名来实现的,策略管理员在配置安全规则时需要先定义好相关的网络地址和端口的别名。

### (2) 设备配置

设备配置是防火墙自身的网络设置,包括对接口设备配置和显示防火墙基本信息。在 FG 初始化完成,以策略管理员身份登录 FC 后,首先需要进行设备配置,用户可以根据自己实际的网络需求在设备配置模块中通过对网络接口的设置实现多种工作模式。

防火墙可以有 3 种工作模式:桥模式、路由模式和混杂模式。

- 桥模式:如果用户不想改变原有的网络拓扑结构和设置,可以将防火墙设置成桥模式。在桥模式下,网络间的访问是透明的,所有网口设备将构成一个网桥。
- 路由模式:是防火墙的基本工作模式。在路由模式下,防火墙的各个网口设备的 IP 地址都位于不同的网段。
- 混杂模式:指防火墙部分网口在路由模式下工作,部分网口在桥模式下工作。即某些子网之间以路由方式通信,而某些子网可以透明通信。

### (3) SNMP 配置

FG 支持 SNMP 简单网络管理协议。一方面,网络管理工具可以实时获取 FG 的状态为其提供相关的系统状态、网络接口状态、IP 状态、ARP 表状态和 SNMP 服务状态等信息。另一方面,FG 为网络管理平台定期提供有关 FG 防火墙的信息,如入侵信息、管理信息和

系统信息。

SNMP 的界面配置可分为 4 个部分：

- 防火墙位置标识：对系统本地位置信息进行配置。
- 共同体(Community)：用于简单的权限控制，默认为 public。
- SNMP 管理服务器地址：网络管理服务器地址。
- 管理服务器 Trap 服务端口：网络管理服务器 Trap 接收端口，默认为 162。

#### (4) 双机热备份技术

双机热备份是指一台 FG 为主机，正常情况下处于工作状态，另一台 FG 作为备用机，平时处于备用状态，并不工作，当工作状态的系统出现故障时，备用状态的防火墙在保证网络的正常使用的前提下，立即自动切换到工作状态，接替主机的角色，承担防火墙的工作。

方御防火墙系统在桥模式下能够在网络中智能地寻找其对等的备份机，并且使备份机自动进入等待状态，而一旦备份机发现主工作机失效，可及时的启动，防止网络中断事故的发生。要保护网络的安全，防火墙本身首先要安全。即使防火墙未被黑客攻击，也会由于问题，原器件老化、异常死机等特殊原因发生故障。一旦发生故障，网络的安全就无法保证。对可靠性要求很高的用户，一定要选用有双机热备份技术的防火墙。FG 在路由模式下的双机热备份需要手工设置。

双机热备份连接示意图如图 6.2 所示，两台 FG 的 COM 2 口需要用串口线连接；两台 FG 的内部、外部、DMZ 区以及控制接口需要分别通过交换机或集线器用网线连接。硬件连接完成后，需要在 FG 控制端进行设置。只有策略管理员可以设置双机热备功能。双机热备份系统只在桥和路由模式下工作，不支持混杂模式及 VLAN。

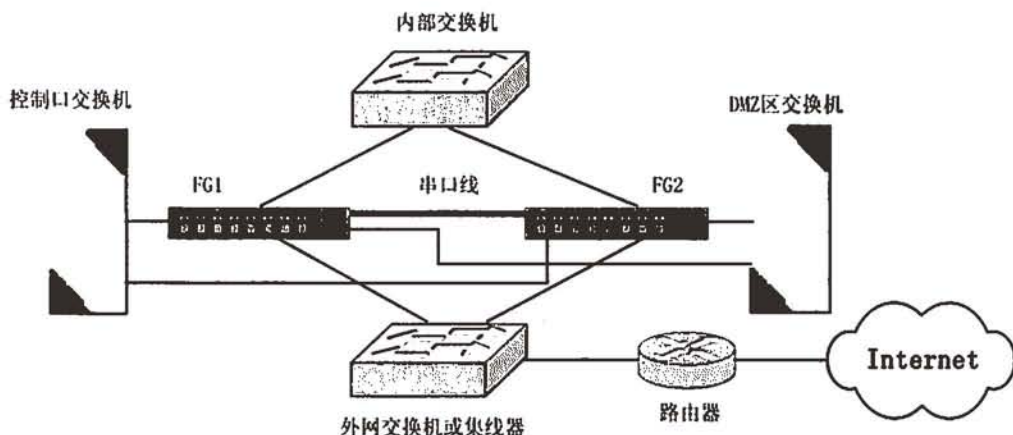


图 6.2 双机热备份连接示意图

### 3. 规则配置

FG 防火墙提供基于状态检测技术的包过滤，能够根据数据包的地址、协议和端口进行访问控制。FG 防火墙包过滤功能主要是通过制定过滤规则集，对数据包头源地址、目的地址和端口号、协议类型等标志进行检查，判定是否允许通过。对于满足过滤规则的数据包，可以选择放过或者丢弃，不满足规则的包则被丢弃。包过滤规则采用按顺序匹配的方式，

即首先匹配前面的规则,若匹配则不再向下执行,因此一定要注意规则设置的顺序问题。

防火墙的规则配置是面向网口设备的,每个网口上的规则是指:每个接口设备接收到的数据包要经过这些规则的过滤,此处的接口包括物理接口设备和 VLAN 设备。每条规则详细描述了源/目的地址、目的端口、协议、数据流向、状态检测和策略等信息。

策略包括 4 种:禁止(DROP)、允许(ACCEPT)、用户认证(AUTH)、自动封禁(AUTO)。

- 允许(ACCEPT):接收此包。
- 禁止(DROP):丢弃此包。
- 自动封禁:FG 启动入侵检测功能后,需要在防火墙模块相应接口设备(包括物理网口、VLAN 设备)上添加一条“自动封禁”规则,才能自动封禁入侵 IP。FG 的每个网口都可以自动封禁。一般情况下,将入侵检测功能的自动封禁设置选择物理网口进行监听。
- 用户认证:对于分配了公网 IP 的内部用户,如果出于安全性考虑目的,管理员希望用户必须通过认证才能访问因特网,则需要在用户管理模块中选择一种认证方式(内置账号认证,或第三方认证),并且在防火墙模块的相应接口设备上(一般是内部网对应的网口)添加一条用户认证规则。

## 6.2.2 典型例题分析

例 1 阅读以下说明,回答问题。

【说明】某公司,对外提供 WWW 服务及 E-mail 和 DNS 服务等,同时对所有员工提供 Internet 服务,其拓扑结构图如图 6.3 所示。

具体网络情况如下:

- (1) 外网(即外部网)接口 S1,地址为 211.156.169.6/30(子网掩码表示由 30 个 1 组成,下同),因特网接口端地址为 211.256.169.5/30。
- (2) 内网(即内部网)接口 E0,地址为 210.45.12.1/24(可用地址空间为 210.45.12.0 这个网段,广播地址为 210.45.12.255)。
- (3) 对外服务器默认网关为 210.45.12.1。
- (4) 内网用户利用代理服务上网(代理服务器 IP 地址为 210.45.12.31/24)。
- (5) 内网用户 IP 地址为 210.45.12.0 网段,子网掩码为 255.255.255.0,网关为 210.45.12.1,代理服务器地址为 210.45.12.31。

随着用户的增多 IP 地址紧缺的矛盾日益突出,同时内部网用户及服务器常遭受黑客的攻击,为解决上述问题,公司决定购置一台方正防火墙。

【问题 1】请给出具体方案(拓扑图)。

【问题 2】简述防火墙的硬件连接。

【问题 3】简述防火墙的配置配策。

分析:(1)可购置一台 3 端口防火墙,为有效保护公司服务器的安全,内部服务器与内部主机分开,将服务器放入 DMZ 区,公司员工接入防火墙的另一个端口的网段。

(2)为解决 IP 地址紧缺,内部员工通过防火墙 NAT 地址转换直接上网,取消代理服务器。



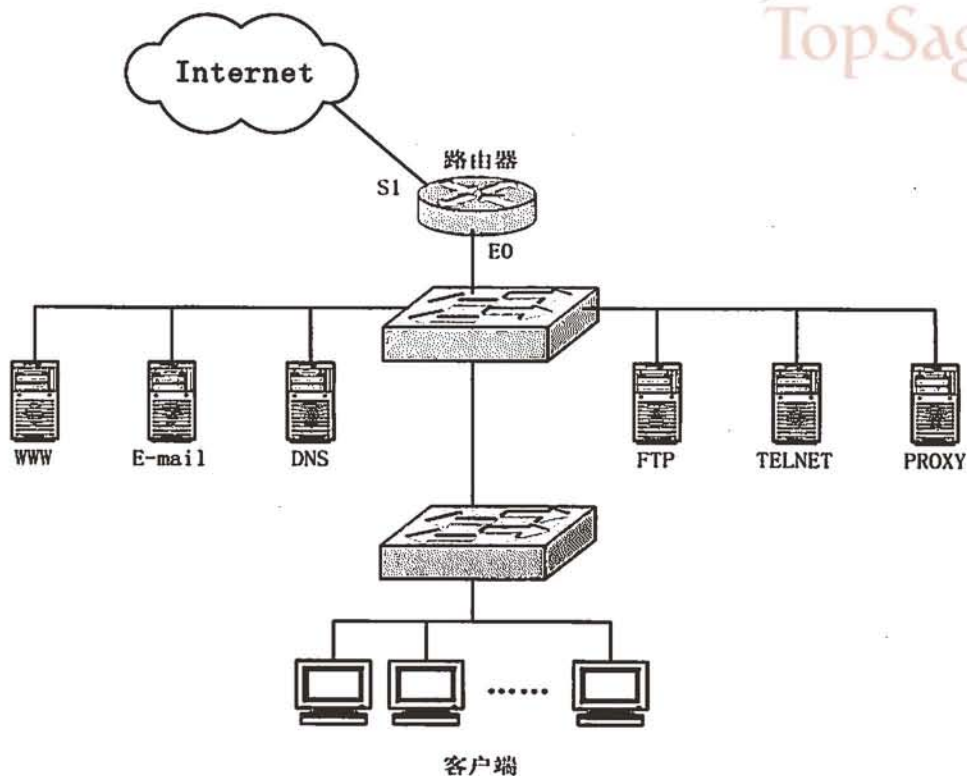


图 6.3 公司网络拓扑结构图

答案:

【问题 1】其连接拓扑结构图如图 6.4 所示。

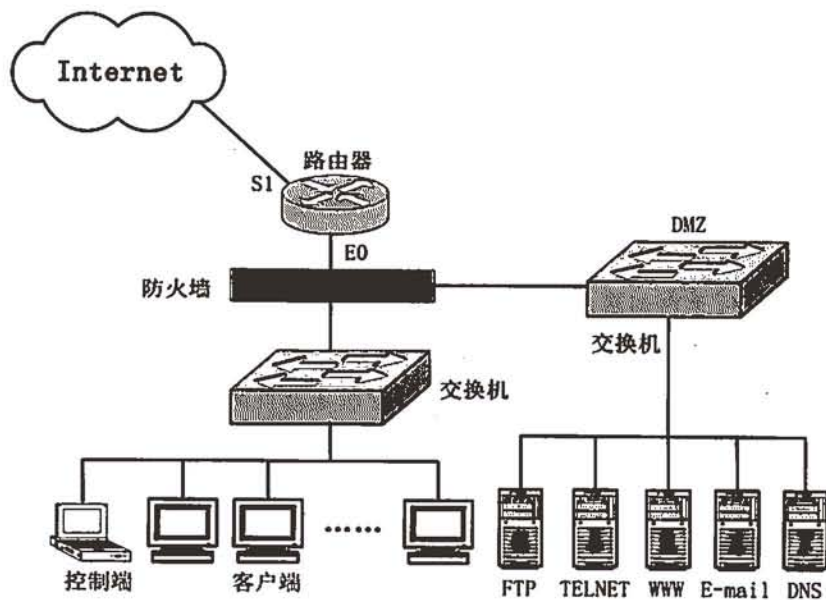


图 6.4 接入防火墙后的网络拓扑图

**【问题 2】硬件连接:**

- 用网线将路由器 E0 端口与 FireGate 的外部接口相连。
- 用网线将内部交换机端口与 FireGate 的内部接口相连。
- 用网线将 DMZ 接口与 DMZ 区交换机相连。
- 用电源线将 FireGate 接上电源, 硬件安装完成。

**【问题 3】配置策略:****(1) 基本配置**

- 防火墙内部接口设为防火墙内部网络接口和管理口, 地址 192.168.1.1/24, 设置好相应的子网掩码后将其选为控制口, 然后提交系统, 使设备配置生效。
- 将 DMZ 区域和外网区域设置为桥, 同时在桥上绑定 IP 地址 210.45.12.31/24(为原代理服务器地址), 配置完成后提交系统, 使设备配置生效。
- 添加内部网、DMZ 区域以及外部网各设备别名。

**(2) 规则配置**

- 按照实际情况配置各种安全措施, 如内部网访问 DMZ 区域 WWW 服务器规则, 内部网访问 DMZ 区域 Telnet 服务器规则等。
- NAT 规则设置。在防火墙设置 NAT 功能实现地址转换, 内部网访问外部 WWW 时, 全部将内部地址转换成防火墙外部网地址 210.45.12.31, 不需要代理服务器。

**例 2** 图 6.5 为某一公司的网络拓扑结构图, 请在图中标出公共网络、内部网络、DMZ 区、内部关键服务器群的位置。

**分析:** 公共网络(非信任网络): 处于防火墙之外的公共开放网络, 一般指 Internet。

内部网络(信任网络): 处于防火墙之内的可信网络, 是防火墙要保护的目标。

DMZ(非军事化区): 也称周边网络, 可以位于防火墙之外也可以位于防火墙之内。安全敏感度和保护强度低。非军事化区一般用来放置提供公共网络服务的设备。这些设备由于必须被公共网络访问, 所以无法提供与内部网主机相等的安全性。

一般用户区: 位于内部网内不具有可信任的主机群。

内部关键服务器群: 内部网内重点保护的服务器。通常与内网一般用户分开。

**答案:** (1)公共网络或 Internet      (2)内部关键服务器群区

(3)DMZ 区

(4)一般用户区

(5)内部网络

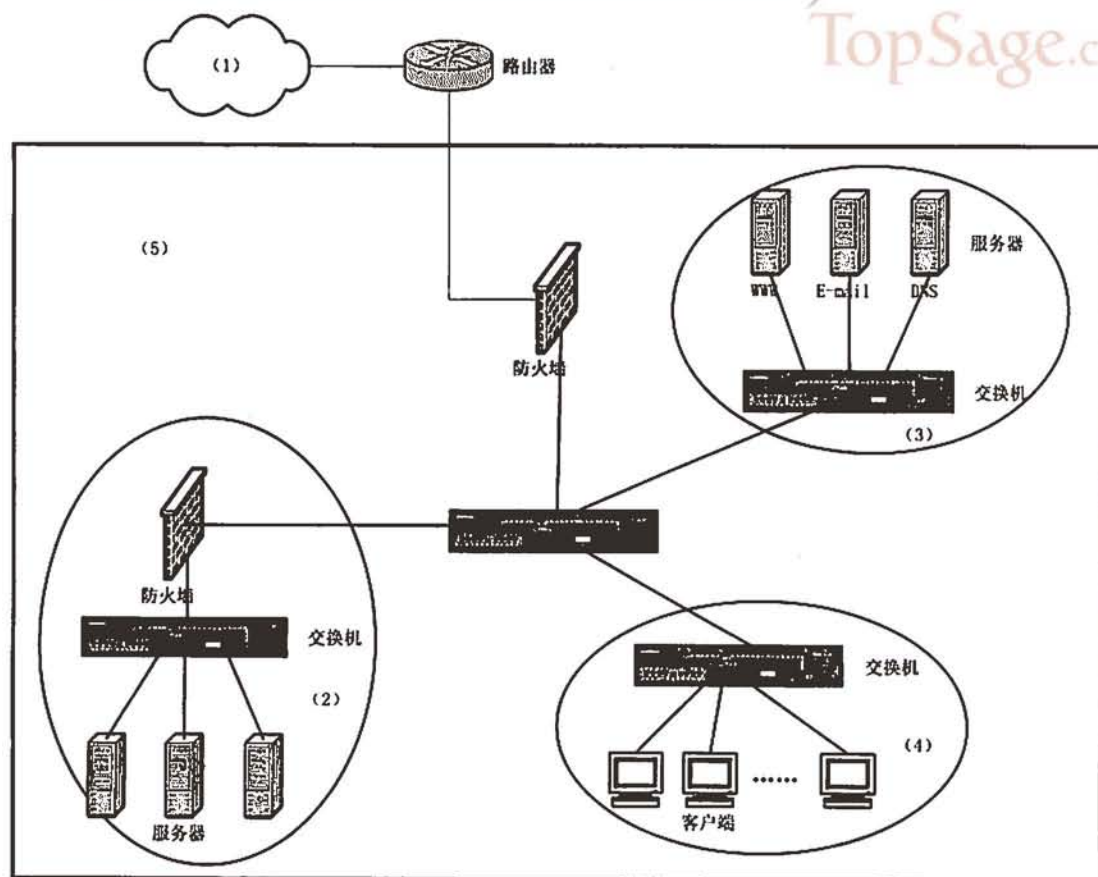


图 6.5 公司网络拓扑结构图

### 6.2.3 同步练习

1. 简述 FireGate 防火墙的三种工作模式。
2. 什么是双机热备份？请画出双机热备份拓扑图并简述其连接。
3. 简述 FireGate 防火墙四种配置策略。

4. 某一小型公司，通过电信光纤接入互联网，同时申请了四个公网 IP 地址，该公司购置一台两端口防火墙用于公司内部人员通过 NAT 地址转换上互联网，公司有一台服务器对外只提供 WEB 服务，为节省资金，该服务器直接接入互联网。请给出其网络安全方案并画出其拓扑结构图。

### 6.2.4 同步练习参考答案

1. 答案见本节考点辅导。
2. 答案见本节考点辅导。
3. 答案见本节考点辅导。
4. (1)服务器设置一个公网 IP 地址，安装软件防火墙，关闭不需要的端口。

(2) 防火墙外网端口设置一个公网 IP 地址, 内网端口设置一保留地址(如, IP 地址 192.168.0.1/24), 内网内客户机设置的地址为 192.168.0.1 网段, 子网掩码为 255.255.255.0, 网关为 192.168.0.1。内网内客户机私有地址即可转换为公网的合法 IP 地址, 实现了 NAT 地址转换上互联网。

(3) 其连接拓扑结构图如图 6.6 所示。

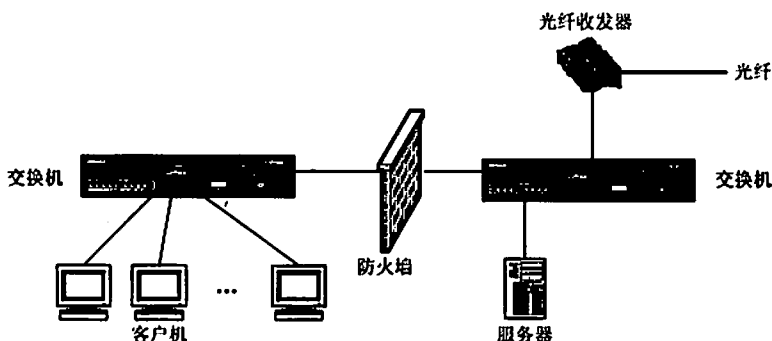


图 6.6 公司网络拓扑结构图

## 6.3 入侵处理策略

### 6.3.1 考点辅导

#### 6.3.1.1 入侵检测系统概述

##### 1. 入侵检测系统

入侵检测系统(IDS)通过从计算机网络或计算机系统的关键点收集信息并进行分析, 从中发现网络或系统中是否有违反安全策略的行为和被攻击的迹象。入侵检测系统可以说是防火墙系统的合理补充和延伸, 如果说防火墙是第一道安全闸门, 入侵检测系统则可以说是第二道安全闸门。入侵检测系统在不影响网络性能的前提下, 实时、动态地保护来自内部和外部的各种攻击, 同时有效地弥补了防火墙所能达到的防护极限。

根据进行入侵分析的数据来源的不同, 可以将入侵检测系统分为基于网络的入侵检测系统(NIDS)和基于主机的入侵检测系统(HIDS)。

基于网络的入侵检测系统(NIDS)的数据来源为网络中传输的数据包及相关网络会话, 通过这些数据和相关安全策略来进行入侵判断。

基于主机的入侵检测系统(HIDS)的数据来源主要为系统内部的审计数据, 通过这些数据来分析、判断各种异常的用户行为及入侵事件。

##### 2. 入侵系统的功能

入侵检测系统的主要功能:

(1) 监测并分析用户和系统的活动。



- (2) 核查系统配置和漏洞。
- (3) 评估系统关键资源 and 数据文件的完整性。
- (4) 识别已知的攻击行为。
- (5) 统计分析异常行为。
- (6) 操作系统日志管理, 并识别违反安全策略的用户活动。

### 3. 入侵检测系统工作流程

通常入侵检测系统为了分析、判断特定行为或事件是否为违反安全策略的异常行为或攻击行为, 需要经过下列四个过程。

#### (1) 信息收集

网络入侵检测系统(NIDS)或者主机入侵检测系统(HIDS)都需要采集必要的用于入侵分析。

#### (2) 数据过滤及缩略

根据预定义的设置, 进行必要的的数据过滤及缩略, 从而提高检测、分析的效率。

#### (3) 信号分析

对收集到的信息, 一般通过三种技术手段进行分析: 模式匹配、统计分析和完整性分析。其中前两种方法用于实时的入侵检测, 而完整性分析则用于事后分析。

#### (4) 报警及响应

一旦检测到违反安全策略的行为或者事件, 进行报警及响应。主要的响应方式有: 记录日志、发出报警声、发送电子邮件通知管理员、切断连接等安全控制。

### 4. 网络入侵检测系统的必要性

防火墙在网络安全中起到防护的作用, 对进出的数据依照预先设定的规则进行匹配, 符合规则的就予以放行, 起访问控制的作用, 是网络安全的第一道闸门。优秀的防火墙甚至能对高层的应用协议进行动态分析, 保护进出数据应用层的安全。但防火墙的功能也有局限性。防火墙只能对进出网络的数据进行分析, 对网络内部发生的事件完全无能为力。

同时, 由于防火墙处于网关的位置, 不可能对进出数据作太多判断, 否则会严重影响网络性能。如果把防火墙比作大门警卫的话, 入侵检测就是网络中不间断的摄像机, 入侵检测通过旁路监听的方式不间断地收取网络数据, 对网络的运行和性能无任何影响, 同时判断其中是否含有攻击的企图, 通过各种手段向管理员报警。不但可以发现从外部的攻击, 也可以发现内部的恶意行为。所以说入侵检测是网络安全的第二道闸门, 是防火墙的必要补充, 是构成完整的网络安全解决方案的必要条件。

#### 6.3.1.2 入侵检测系统部署

##### 1. 部署实例

对于入侵检测系统来说, 其类型不同、应用环境不同, 部署方案也会有所差别。对于基于主机的入侵检测系统来说, 它一般用于保护关键主机或服务器, 因此只要将它部署到这些关键主机或服务器中即可。但是基于网络的入侵检测系统来说, 各种网络环境千差万别, 根据网络环境的不同, 其部署方案也会有所不同。

### (1) 共享部署

在共享介质的环境下, 传感器能够监听到整个冲突域内的流量, 所以只需要把传感器的监听端口接到 Hub 上即可, 如图 6.7 所示。

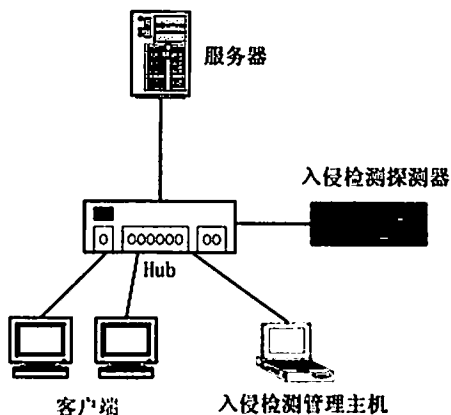


图 6.7 共享介质环境入侵检测下的部署

### (2) 交换环境

在交换环境下, 每个交换机的端口都是一个独立的冲突域, 因此传感器不能直接监听到交换机其他端口的流量, 通常可以采用以下几种方法解决:

- 在交换机和路由器之间接入一个 Hub, 从而把一个交换环境转换为共享环境。这样做的优点是简单易行, 成本低廉。如果客户对网络的传输速度和可靠性要求不高, 建议采用这种方法, 如图 6.8 所示。

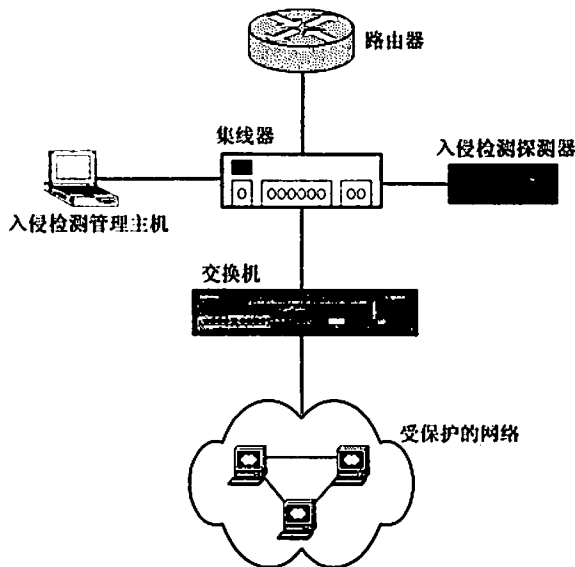


图 6.8 交换环境下接入集线器入侵检测部署

- 如果交换机支持端口镜像的功能, 建议采用这种方法, 可以在不改变原有网络拓扑结构的基础上完成传感器的部署, 配置简单、灵活, 使用方便, 不需中断网络,

是比较常用的一种方式,如图 6.9 所示。

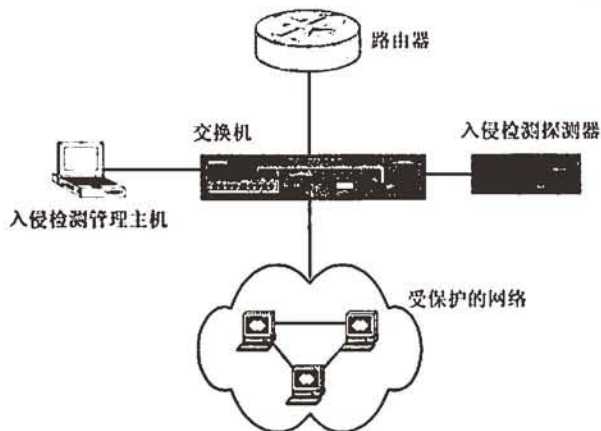


图 6.9 交换环境下入侵检测部署

- 如果交换机不支持端口镜像功能,或者出于性能的考虑不便启用该功能,可以采用 TAP(分支器),它的优点是能够支持全双工 100Mb/s 或者全双工 1000Mb/s 的网络流量。

## 2. 典型应用

本实例假设所采用的交换机支持端口镜像的功能。

### (1) 小规模网络环境

此种区域网连接方法较为简单,内部网络中各机构的主机使用共享式 Hub 连接到交换机上,或主机直接连接到交换机上,交换机不设 VLAN,交换机再通过路由器接入 Internet。在这种情况下,将 IDS 监测主机接到交换机的广播口(监听口)即可监听到内部网络间的所有通信及内部网络到 Internet 的所有通信,如图 6.10 所示。

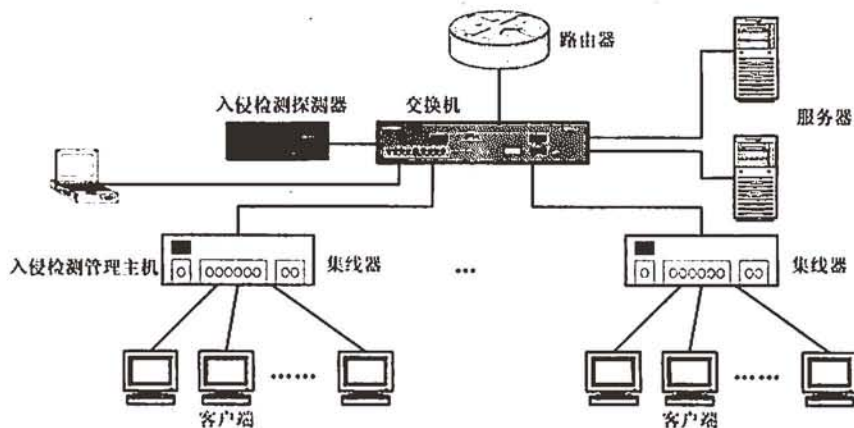


图 6.10 小规模网络环境应用图

### (2) 分布式监测应用示例

网络结构相对较复杂,内部网络中各机构间使用交换机连接到主交换机上,通过主交换机连接路由器接入 Internet。此时,在主交换机的广播口(监听口)上无法监听到从交换机

上的机器间的通信，为了全面监控网络，捕捉内部网间的恶意攻击与入侵行为，就需要为每个重要的网段部署一个入侵检测探测器，并分别将检测到的事件发送到集中管理控制台，如图 6.11 所示。

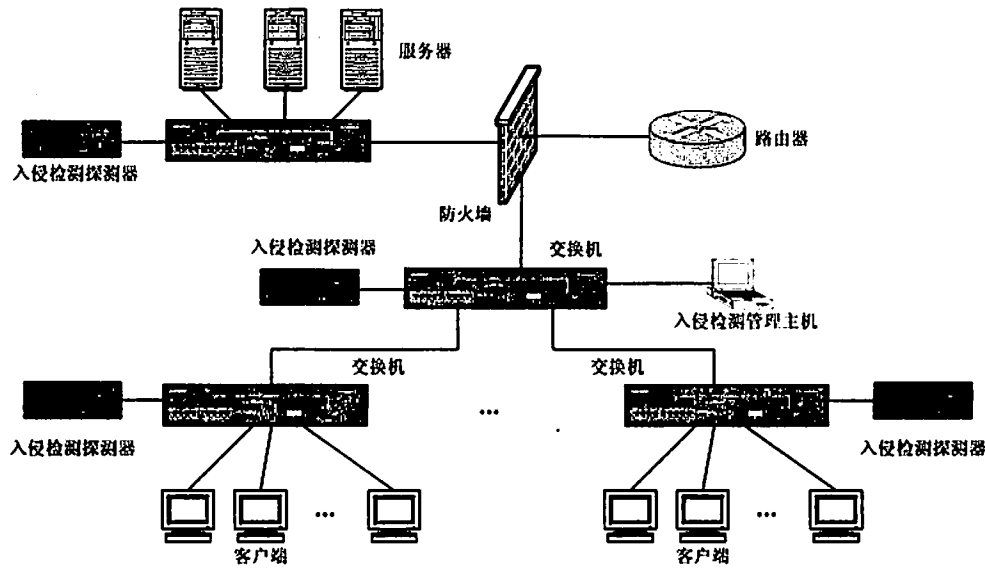


图 6.11 多子网分布式环境应用图

6.3.2 典型例题分析

例 阅读以下说明，回答问题。

【说明】

图 6.12 为某公司的拓扑结构图，该公司最主要的应用系统包括 WWW、E-mail、DNS 系统以及内部办公自动化系统、数据库及备份系统等。该公司对信息数据的保密性和安全性一直都比较重视，所以在网络中部署了 1 台防火墙，虽然公司对安全风险有所防范，但是实际情况还是不尽如人意，网络依然遭受破坏和干扰，企业业务也因此受到了严重的影响，损失很大。

经网络安全专家“诊断”发现该公司的防火墙配置比较简单、管理过于宽松，像没有用到的 135~142 端口处于开放状态，IP 地址与 MAC 地址之间也没有被绑定；文件共享设置十分混乱，有几台服务器的 C 盘(含有系统文件)能被内网上的用户任意访问，IIS Web Server 未进行最新的软件补丁等。以上问题足以使内部或外部的人员发生误操作或进行有如基于 IPC 的远程控制、IP 地址盗用或基于 Web 的 Unicode 攻击和 Printer 攻击等。其次，该公司缺乏对自身网络实际安全状况的了解。比如某些应用系统存在很多 Bug，某些设备(比如防毒产品和防火墙等)配置过于粗糙。

通过以上“诊断”，网络安全专家认为该企业的主要需求可概括为以下几点。

- 需要对主要网段进行监控，以随时发现网络内部的攻击、入侵、可疑或其他非授权的行为。
- 需要对关键主机进行保护和监控，以随时反映主机上系统活动状态或日志信息。



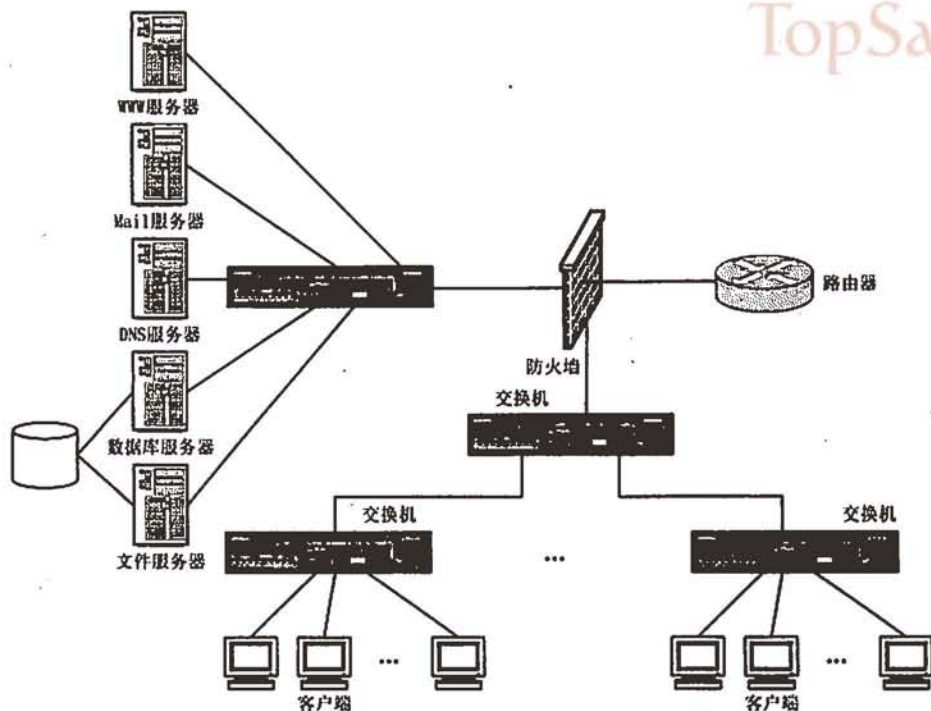


图 6.12 公司拓扑结构图

- 需要对各种非正常的网络事件或主机事件做记录或跟踪，而对于一些非法或恶意的连接则要及时做出响应(如中断它们的 TCP 会话等)。
- 需要集中统一的控制平台。
- 需要定期检查自身网络的安全状况，提前发现网络中的脆弱性，及时采取调整或修补措施。

根据以上分析请回答以下问题：

【问题 1】为什么在企业内部布署了防火墙，还要布署入侵检测产品。

【问题 2】请给出入侵检测产品布署方案(拓扑结构图)。

分析：

(1) 按照网段或主机对安全等级的要求，选择在最重要的对象上进行 IDS 部署，以确保关键网段和关键主机的安全。采用动态检测、实时记录、及时报警和主动防御的动态检测防护系统。

(2) 以防火墙为界线，内部网形成了 2 个主要的网段，其中，服务器群是最重要的网段。因此，分别在防火墙后面安装 1 台基于网络的网络探测器(NIDS)，以监控 2 个网段上的网络数据流，及时发现网络上的攻击行为。

(3) 从服务应用的重要性来看，WWW 服务器、Mail 服务器、DNS 服务器、数据库服务器及文件服务器是最需要被特别保护的，因而又分别安装基于主机的主机探测器(HIDS)，以随时监视本地系统上的系统活动事件和日志信息。

(4) 在网络控制中心的管理机上安装了网络实时监控软件，以使网管人员对 NIDS 和 HIDS 进行集中的管理和控制。

(5) 如此部署以后,一旦网络上或主机上的探测器探测到危险的事件发生,探测器将立即发出报警,报警信息可以通过发送文字、传真、E-mail、手机短信息等各种手段通知系统管理员,网络监控主机将所有的报警信息记到日志中,以备核查。同时探测器还能够针对恶意攻击进行实时响应。

(6) 管理员收到报警后可以查询和推断事件的原因、依据日志信息调查过去的相关历史情况、定位非法工作站和跟踪取证或清除连接。

答案:

【问题 1】防火墙有许多局限性,如防火墙不能防范不经过防火墙的攻击、防火墙不能解决来自于内部网络的攻击和安全问题、防火墙不能防止最新的未设置策略或错误配置引起的安全威胁、防火墙不能防止可接触的人为或自然的破坏、防火墙无法解决 TCP/IP 等协议的漏洞、防火墙对服务器合法开放的端口的攻击大多无法阻止、防火墙不能防止受病毒感染的文件的传输、防火墙不能防止数据驱动式的攻击、防火墙不能防止内部的泄密行为、防火墙不能防止本身安全漏洞的威胁。同时它又处于网关的位置,不可能对进出攻击作太多判断,否则会严重影响网络性能。如果把防火墙比作大门警卫的话,入侵检测就是网络中不间断的摄像机,入侵检测通过旁路监听的方式不间断的收取网络数据,对网络的运行和性能无任何影响,同时判断其中是否含有攻击的企图,通过各种手段向管理员报警。不但可以发现从外部的攻击,也可以发现内部的恶意行为。所以说入侵检测是网络安全的第二道闸门,是防火墙的必要补充,构成完整的网络安全解决方案。

【问题 2】根据要求其入侵检测部署拓扑结构图,如图 6.13 所示。

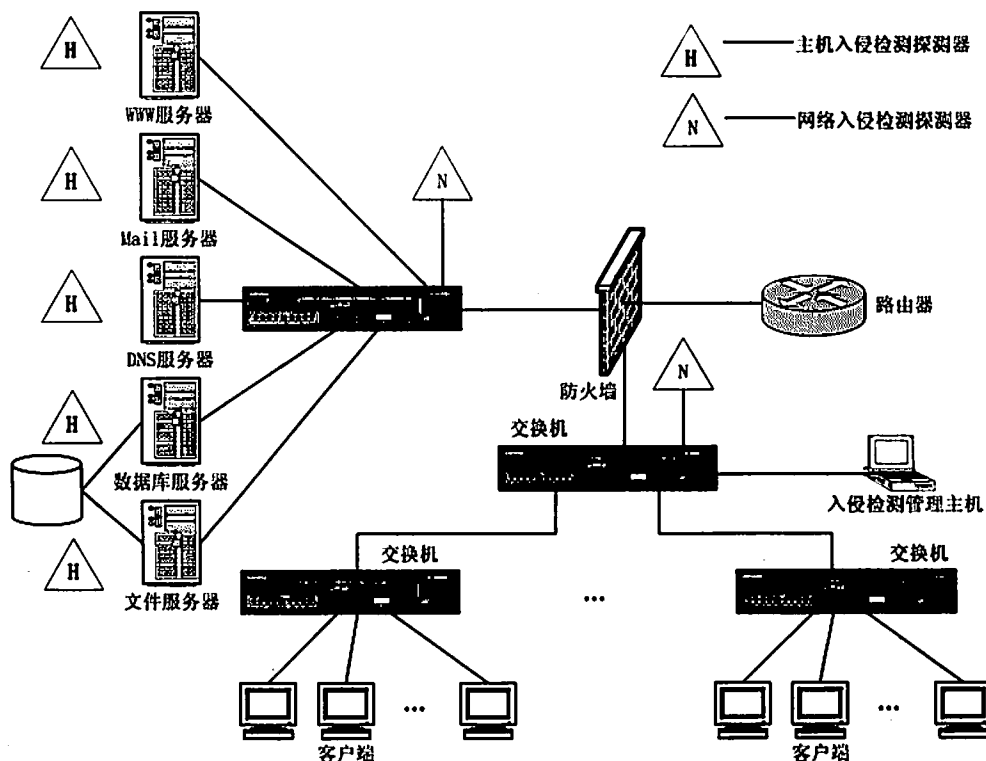


图 6.13 具有入侵检测功能网络拓扑结构图

### 6.3.3 同步练习

1. 通常,入侵检测系统为了分析、判断特定行为或者事件是否为违反安全策略的异常行为或者攻击行为,需要经过4个过程。请在图6.14中分别填写出这4个过程。

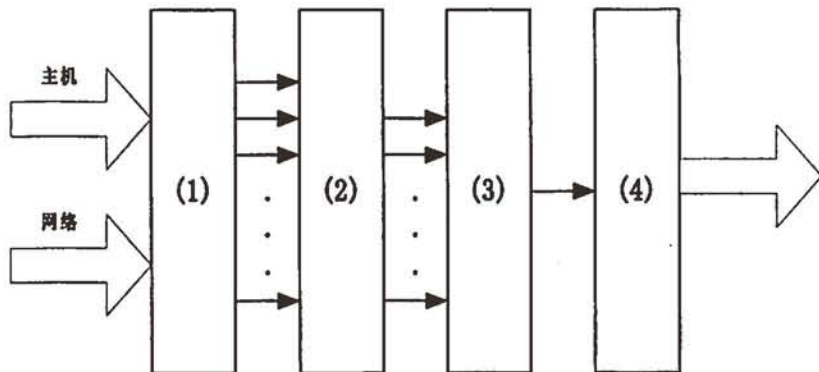


图 6.14 入侵检测系统工作流程图

2. 对于不同的网络结构和应用目的,入侵检测系统安装方式和策略配置都应当有所不同。请给出 Hub 与交换机(支持端口镜像的功能)入侵检测连接拓扑结构图。

### 6.3.4 同步练习参考答案

- (1)信息收集 (2)数据过滤及缩略 (3)信号分析 (4)报警及响应
- Hub 与交换机(支持端口镜像的功能)入侵检测连接拓扑结构图,如图 6.15 所示。

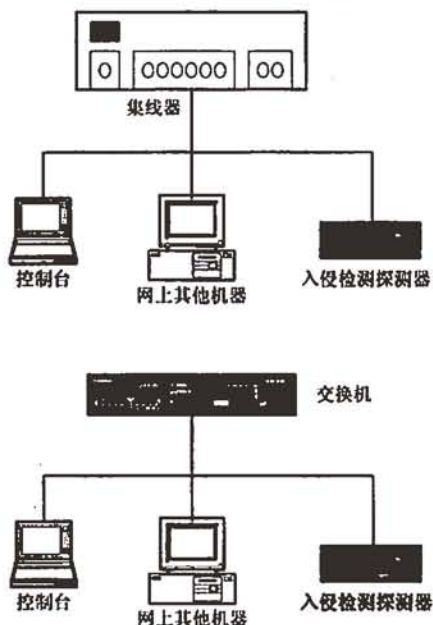


图 6.15 入侵检测系统应用图

## 6.4 漏洞处理策略

### 6.4.1 考点辅导

#### 6.4.1.1 漏洞扫描系统简介

漏洞扫描系统是一种自动检测远程或本地主机安全性弱点的程序，是检测远程或本地系统安全脆弱性的一种安全技术。

#### 6.4.1.2 进行网络扫描的必要性

随着企业网络的日趋扩大、日趋动态化和日趋复杂，发现严重安全性威胁的可能性也呈指数增长。网络扫描系统可根据企业提供网络服务进行风险评估，同时它可在那些常见安全漏洞被入侵者利用并实施攻击之前，就识别出这些漏洞，从而帮助企业妥善保护系统和网络。网络系统的安全性取决于网络系统中最薄弱的环节。如何及时发现网络系统中最薄弱的环节？如何最大限度地保证网络系统的安全？最有效的方法是定期对网络系统进行安全性分析，及时发现并修正动态运行的网络系统中存在的弱点和漏洞，如 WWW 服务中的信息泄露、缓存区溢出漏洞，FTP 匿名服务的安全漏洞，Sendmail 安全漏洞等，正是这些安全漏洞和不安全配置会给入侵者以可乘之机，他们会利用这些安全漏洞和不安全的设置对网络进行恶意的入侵和破坏，使企事业单位蒙受巨大损失。

网络扫描系统正是这样的一套能够帮助您实现网络系统安全，为您解决后顾之忧的有效安全检测工具。网络扫描系统能全面地检查服务器、路由器、防火墙、操作系统和网络应用进程，最大限度地保证网络系统的安全。

#### 6.4.1.3 漏洞扫描工具

在网络安全策略的引导下，对网络可能存在的安全漏洞进行扫描，预先评估网络的安全性能，提供详细的网络安全隐患报告，找出网络的安全漏洞，给出网络漏洞修补建议是提高网络安全的重要措施，是保持网络安全的积极防御手段。网络漏洞扫描系统作为网络安全性的评估工具，一直受到网络安全产品提供商的重视，研发了具有不同特点的漏洞扫描工具。

漏洞扫描工具主要是静态对网络中的各种系统、设备和数据库进行漏洞扫描，找出整个网络系统中最容易受到攻击的地方，对网络进行有效的评估，最后提出建设性的解决方案。其工作原理是采用模拟攻击的形式对目标可能存在的已知安全漏洞进行逐项检查。目标可以是工作站、服务器、交换机、数据库应用等各种对象。漏洞扫描工具可以分为三种：基于服务器的扫描器、基于网络的扫描器和基于数据库的扫描器，分别可以对服务器、网络及数据库的安全漏洞进行扫描并提出安全分析报告。

#### 6.4.1.4 漏洞处理策略

漏洞形成的原因形形色色、不一而足，最常见的漏洞主要包含以下类型：CGI 脚本、



POP3、FTP、SSH、HTTP、SMTP、IMAP、后门、RPC、DNS 漏洞等。根据不同的漏洞类型会有不同的漏洞处理策略。

### 6.4.2 典型例题分析

**例** 请给出漏洞扫描系统应用案例(拓扑结构图)。

**分析:** 漏洞扫描系统应用的基本原则: 当漏洞扫描系统服务器能够与待测目标和系统客户端之间互相通信时, 系统服务器才能对目标进行检测, 否则将无法检测目标漏洞。

**答案:** 如图 6.16 所示, 架设两台漏洞扫描服务器, 服务器 1 的架设需要能访问内网中的所有子网并负责内部子网的扫描。服务器 2 架设在 DMZ 区, 负责对该区的服务器的扫描检测工作。同时漏洞扫描系统根据攻击技术的发展可及时更新升级, 升级过程是通过 Internet 网直接从厂家提供的技术支持服务网站上下载。

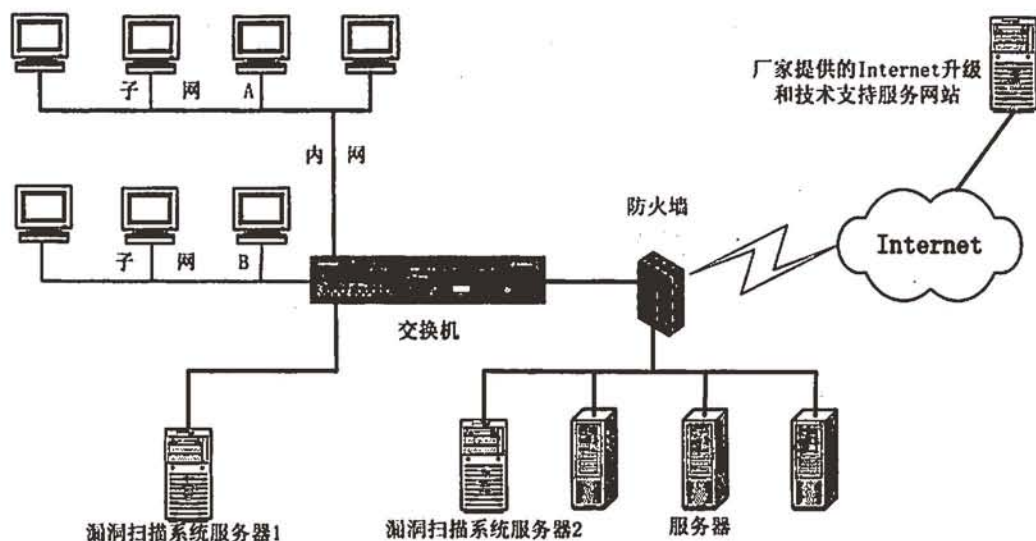


图 6.16 漏洞扫描系统布置图

### 6.4.3 同步练习

1. 对于 CGI 脚本的缓冲区溢出攻击、数据验证型溢出攻击、信息泄漏, 其解决方案是什么?
2. SMTP 是简单邮件传输协议, 其服务守护程序是 Sendmail, 如何解决 Sendmail 中的漏洞?

### 6.4.4 同步练习参考答案

1. 缓冲区溢出攻击解决方案: 修改 CGI 脚本, 加入对“\n”的检验, 或者暂停使用该脚本。

数据验证型溢出攻击解决方案: 考虑利用正则表达式增加输入验证, 过滤诸如../和../之类的字符组合, 也可以增加一个变量限制目录遍历深度。结合这两种技术, 就可以限制

来自潜在攻击者的任意目录遍历行为。

信息泄漏解决方案：在浏览器中禁止 Java Applet。

2. 升级到高版本 Sendmail。

## 6.5 本章小结

本章主要介绍了网络病毒防护策略、防火墙的配置策略、入侵处理策略、漏洞处理策略。

要求考生掌握网络病毒防护、防火墙、入侵处理、漏洞处理的基本概念，熟悉在不同网络环境下的部署及网络安全解决方案。

## 6.6 达标训练题及参考答案

### 6.6.1 达标训练题

阅读以下说明，回答问题。

某学校的拓扑结构图如图 6.17 所示，为加强网络安全，学校决定购置一台三端口防火墙保护内部网络；购置了入侵检测产品对重点网段和服务器进行监控；购置一套网络版杀毒软件(Server 版)并安装于一台服务器上，客户端、服务器通过防病毒服务器提供的 Web 页面自动下载安装并具有自动跟踪防病毒服务器更新病毒库的功能。

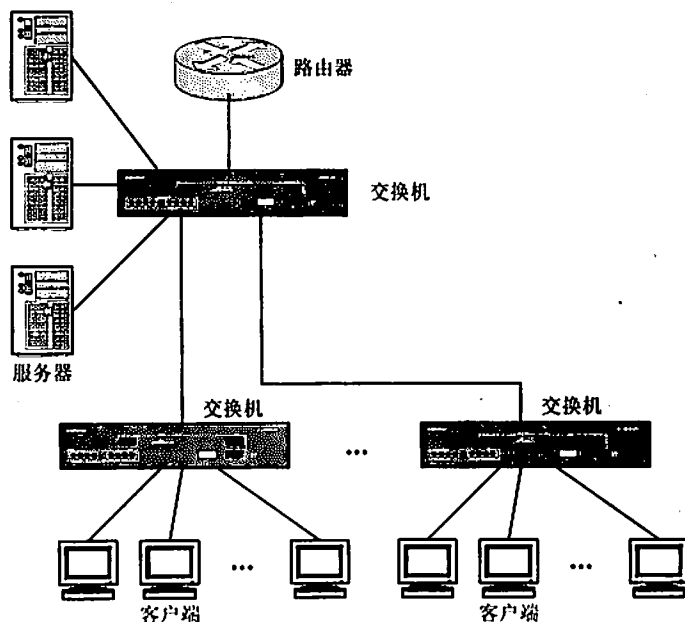


图 6.17 某校园网拓扑结构图

【问题 1】什么是防火墙？简述其功能及优点？

【问题 2】什么是入侵检测？简述其功能？

【问题 3】什么是网络病毒？简述其特点？对防病毒服务有什么要求。

【问题 4】请给出该网络的安全方案(拓扑结构图)，并在图中标出相应设备的名称。

## 6.6.2 参考答案

【问题 1】防火墙是位于两个信任程度不同的网络之间的软件或硬件设备的组合，它对两个或多个网络之间的通信进行控制，通过强制实施统一的安全策略，防止对重要信息资源的非法存取和访问，以达到保护系统安全的目的。其功能与特点有：

- 对进出的数据包进行过滤，过滤掉不安全的服务和非法用户。
- 监视 Internet 安全，对网络攻击行为进行检测和报警。
- 记录通过防火墙的信息内容和活动。
- 控制对特殊站点的访问，封堵某些禁止的访问行为。
- 防火墙能强化安全策略。
- 防火墙能有效的记录 Internet 上的活动。
- 防火墙是一个安全策略的边防站。

【问题 2】入侵检测系统(IDS)通过从计算机网络或计算机系统的关键点收集信息并进行分析，从中发现网络或系统中是否有违反安全策略的行为和被攻击的迹象。入侵检测系统可以说是防火墙系统的合理补充和延伸，如果说防火墙是第一道安全闸门，入侵检测系统则可以说是第二道安全闸门。入侵检测系统在不影响网络性能的前提下，实时、动态地保护来自内部和外部的各种攻击，同时有效地弥补了防火墙所能达到的防护极限。入侵检测系统的主要功能：

- 监测并分析用户和系统的活动。
- 核查系统配置和漏洞。
- 评估系统关键资源和数据文件的完整性。
- 识别已知的攻击行为。
- 统计分析异常行为。
- 操作系统日志管理，并识别违反安全策略的用户活动。

【问题 3】网络病毒在网络上传播的计算机病毒，为网络带来灾难性后果，被称之为“第二代病毒”。网络病毒的特点及危害性主要表现在：破坏性强、传播性强、具有潜伏性和可激发性、针对性更强、扩展面广、传播速度快、难以彻底清除。

要求防病毒服务器每天下载并更新病毒定义库。

【问题 4】其配置拓扑结构图如图 6.18 所示。

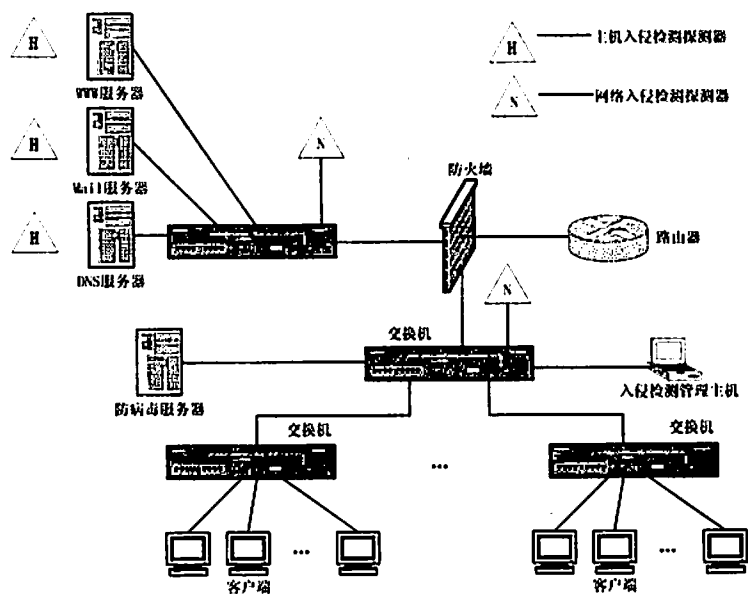


图 6.18 网络安全解决拓扑结构图



## 参 考 文 献

1. 全国计算机技术与软件专业技术资格(水平)考试办公室编. 网络管理员考试大纲. 北京: 清华大学出版社, 2004
2. 张国鸣主编. 网络管理员教程. 北京: 清华大学出版社, 2004
3. 雷震甲主编. 网络工程师教程. 北京: 清华大学出版社, 2004
4. Andrew S.Tanenbaum 著, 熊桂喜等译. 计算机网络(第3版). 北京: 清华大学出版社, 2001
5. 谢希仁编著. 计算机网络(第4版). 北京: 电子工业出版社, 2003
6. 施威铭研究室著. Red Hat Linux 7.2 架设实务. 北京: 清华大学出版社, 2003
7. 梁如军编著. Red Hat 7.0 安装配置与管理. 北京: 清华大学出版社, 2001
8. 只飞, 窦丽芳等编著. Windows 2003 系统管理. 北京: 清华大学出版社, 2004
9. 张凤琴, 张国鸣主编. 网络管理员考试辅导. 西安: 西安电子科技大学出版社, 2004
10. 郑若忠主编. 全国计算机技术与软件专业技术资格(水平)考试(网络管理员分册). 北京: 中国水利水电出版社, 2004
11. 李怀强主编. 全国计算机等级考试考点与题解. 北京: 中国经济出版社, 2002
12. 全国计算机等级考试命题研究组编著. 全国计算机等级考试考点分析、题解与模拟(三级网络技术). 北京: 电子工业出版社, 2004
13. 雷建军主编. 计算机网络实用技术. 北京: 中国水利水电出版社, 2001
14. 邱平主编. 局域网技术与组网工程自学考试指导与题解. 北京: 知识出版社, 2002
15. 杨晓晖编著. 局域网技术与组网工程自学辅导. 武汉: 华中科技大学出版社, 2002
16. 张淑珍, 马恕主编. 局域网技术与组网工程自考应试指导. 南京: 南京大学出版社, 2004
17. 尚晓航编著. 计算机网络与 Windows 2000 实用教程. 北京: 清华大学出版社, 2003
18. 张宏等编著. 网络安全基础. 北京: 机械工业出版社, 2004
19. 薛静锋等编著. 入侵检测技术. 北京: 机械工业出版社, 2004
20. 黄明主编. 全国计算机等级考试考试要点、题解与模拟试卷(三级网络技术). 北京: 电子工业出版社, 2002
21. 王爱英编著. 计算机组成与结构. 北京: 清华大学出版社, 1994
22. 汤子瀛, 哲凤屏, 汤小丹编著. 计算机操作系统. 西安: 西安电子科技大学出版社, 1996
23. 刘兆毓编著. 计算机英语. 北京: 清华大学出版社, 1996
24. 崔巍编著. 数据库系统及应用. 北京: 高等教育出版社, 1999
25. 位元文化编著. JSP 动态网页入门实务. 北京: 科学出版社, 2003
26. Behrouz A.Forouzan, Sophia Chung Fegan 著, 谢希仁译. TCP/IP 协议族. 北京: 清华大学出版社, 2003
27. <http://cdf.51.net/software/nettec/dlfdwq.htm>
28. <http://www.linuxaid.com.cn/engineer/wushubin/html/dhcp.html>
29. [http://www.lib.szu.edu.cn/szulibhtm/ad\\_xkzt/bd\\_txyzd/netsafe/safetechnology/beifen.htm](http://www.lib.szu.edu.cn/szulibhtm/ad_xkzt/bd_txyzd/netsafe/safetechnology/beifen.htm)

# 全国计算机技术与软件专业资格(水平)考试真题及答案

[2008年下半年试题分析与解答 软考指定用书 清华出版](#)(含各科)

[2008年上半年试题分析与解答 软考指定用书 清华出版](#)(含各科)

[2007年下半年试题分析与解答 软考指定用书 清华出版](#)(含各科)

[2007年上半年试题分析与解答 软考指定用书 清华出版](#)(含各科)

[2006年下半年试题分析与解答 软考指定用书 清华出版](#)(含各科)

[2006年上半年试题分析与解答 软考指定用书 清华出版](#)(含各科)

[2009年计算机技术与软件水平考试各科目考试大纲汇总](#)

[全国计算机技术与软件专业资格\(水平\)考试真题及答案汇总](#)

[\[软考视频\]计算机技术与软件专业资格考试推荐视频教程下载汇总](#)

教材及同步辅导见下页。

# 计算机技术与软件专业技术(水平)考试指定教材及同步辅导

## 软考初级:

[程序员教程\(第二版\)2007 版 软考指定用书 高清PDF版](#)

[程序员考试辅导: 全国计算机技术与软件专业技术资格\(水平\)考试辅导用书](#)

[网络管理员教程\(第 2 版\)2007 版 软考指定用书 高清PDF版](#)

[网络管理员考试同步辅导\(计算机与网络基础知识篇\) 软考指定辅导用书](#)

[网络管理员考试同步辅导\(网络系统管理与维护篇\) 软考指定使用辅导用书](#)

## 软考中级:

[网络工程师教程\(第 2 版\) 2007 版 软考指定用书 高清PDF版](#)

[网络工程师教程 软考指定用书 高清PDF版](#)

[网络工程师考试同步辅导: 计算机与网络知识篇 软考指定用书](#)

[网络工程师考试同步辅导\(网络系统设计与管理篇\) 软考指定辅导用书](#)

[软件设计师教程\(第 2 版\) 2007 版 软考指定用书 高清PDF版](#)

[软件设计师考试同步辅导\(下午科目\) 高清PDF版](#)

[软件设计师考试同步辅导\(上午科目\) 高清PDF版](#)

[软件设计师考试考点分析与真题详解\(软件设计技术篇\)](#)

[软件设计师考试辅导: 考点精讲、例题分析、强化训练 冶金工业出版](#)

[数据库系统工程师教程 软考指定用书 高清PDF版](#)

[软件评测师教程 软考指定教材 高清PDF版](#)

[信息系统管理工程师教程 软考指定用书 高清PDF版](#)

[信息系统监理师教程 软考指定用书 高清PDF版](#)

软考高级：

[系统分析师教程 软考指定教材 高清PDF版](#)

[系统分析师考试辅导\(2007 版\) 软考指定辅导用书 高清PDF版](#)

[系统分析师教程 PDF文字版](#)

[系统分析师经典教材 Word版](#)

[信息系统项目管理师教程 软考指定教材 高清PDF版](#)

[信息系统项目管理师辅导教程\(上下册\)](#)

[计算机专业英语教程 PDF文字版](#)

更多计算机资料请访问：[大家论坛计算机专区](#)



# 全国计算机技术与软件专业技术资格（水平）考试参考用书

根据人事部、信息产业部文件，计算机技术与软件专业技术资格（水平）考试纳入全国专业技术人员职业资格证书制度的统一规划。通过考试获得证书的人员，表明其已具备从事相应专业岗位工作的水平和能力，用人单位可根据工作需要从获得证书的人员中择优聘任相应专业技术职务（技术员、助理工程师、工程师、高级工程师）。计算机技术与软件专业实施全国统一考试后，不再进行相应专业技术职务任职资格的评审工作。

## 本系列推荐书目

程序员考试同步辅导（计算机软硬件基础知识篇）

程序员考试同步辅导（程序设计篇）

网络管理员考试同步辅导（计算机与网络基础知识篇）

网络管理员考试同步辅导（网络系统管理与维护篇）

网络工程师考试同步辅导（计算机与网络知识篇）

网络工程师考试同步辅导（网络系统设计与管理篇）

ISBN 7-302-11503-6



9 787302 115038 >

定价：34.00元